TP-LINK®

User Guide

TD-8816B

ADSL2/2+ Ethernet Router



Rev: 1.0.1

1910010017

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. TP-LINK® is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2008 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

http://www.tp-link.com

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to pro-vide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not in-stalled and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.

2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Package contents

The following contents should be found in your package:

- One TD-8816B ADSL2/2+ Ethernet Router
- One AC power Adapter for TD-8816B ADSL2/2+ Ethernet Router
- Quick Installation Guide
- One RJ45 cable
- Two RJ11 cables
- One Resource CD , including:
  - This User Guide
  - Other Helpful Information

☞ **Note:**

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

CONTENTS

Chapter 1. Introduction

1.1 Product Overview

Thank you for choosing the **TD-8816B ADSL2/2+ Ethernet Modem**. The device is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet network.

The Router is easy to use. The TD-8816B connects to an Ethernet LAN or computers via standard Ethernet ports. The ADSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet using a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, **IP/MAC Filter**, **Application Filter** and **URL Filter** can help to protect your network from potentially devastating intrusions by malicious agents from the outside of your network.

The Router is easy to install and manage. **Quick Start** of the Web-based Utility is supplied and friendly help messages are provided for the configuration. Network and Router management is done through the Web-based Utility which can be accessed through local Ethernet using any web browser.

ADSL

The TD-8816B supports full-rate ADSL2+ connectivity conforming to the ITU and ANSI specifications. In addition to the basic DMT physical layer functions, the ADSL2+ PHY supports dual latency ADSL2+ framing (fast and interleaved) and the I.432 ATM Physical Layer.

1.2 Main Features

- One 10/100M RJ-45 LAN ports (Auto MDI/MDIX), 1 RJ11 port
- Downstream data rates up to 24Mbps, upstream data rates up to 3.5Mbps（With Annex M enabled）.
- Supports long transfers, the max line length can reach to 6.5Km.
- Supports remote configuration and management through SNMP and CWMP.
- Supports PPPoE, it allows connecting the internet on demand and disconnecting from the Internet when idle.
- Quick response semi-conductive surge protection circuit, provides reliable ESD and surge-protect function.
- High speed and asymmetrical data transmit mode, provides safe and exclusive bandwidth.
- Supports All ADSL industrial standards.
- Compatible with all mainstream DSLAM (CO).
- Provides integrated access of internet and route function which face to SOHO user.
- Real-time Configuration and device monitoring.

- Supports Multiple PVC (Permanent Virtual Circuit).
- Built-in DHCP server.
- Built-in firewall, supports IP/MAC filter, Application filter and URL filter.
- Supports Virtual Server, DMZ host and IP Address Mapping.
- Supports Dynamic DNS, UPnP and Static Routing.
- Supports system log and flow Statistics.
- Supports firmware upgrade and Web management.

1.3 Conventions

The Router or device mentioned in this User guide stands for TD-8816B without any explanations. Parameters provided in the pictures are just references for setting up the product, which may differ from the actual situation.

Chapter 2. Hardware Installation

2.1 The Front Panel

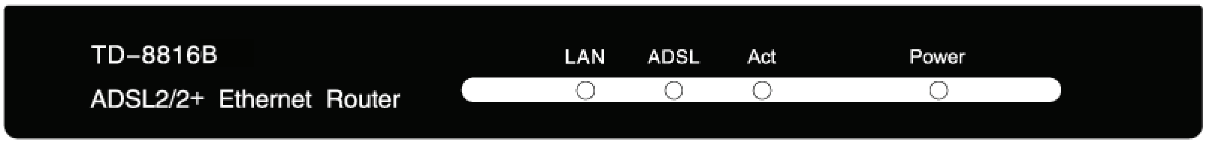


Figure 2-1

The LEDs locates on the front panel, they indicate the device's working status. For details, please refer to LED Explanation.

LED Explanation:

Name	Status	Indication
LAN	On Off Flash	LAN port normal Connection on LAN port abnormal Data transmitting or receiving on LAN port
ADSL	Slow flash Quick flash On	Connection to telecom network is abnormal Connecting to the telecom network Connection to telecom network is OK
ACT	Flash Off	There is data transmitting or receiving on WAN port No data transmitting or receiving on WAN port
Power	On Off	Power OK Power fail

2.2 The Back Panel

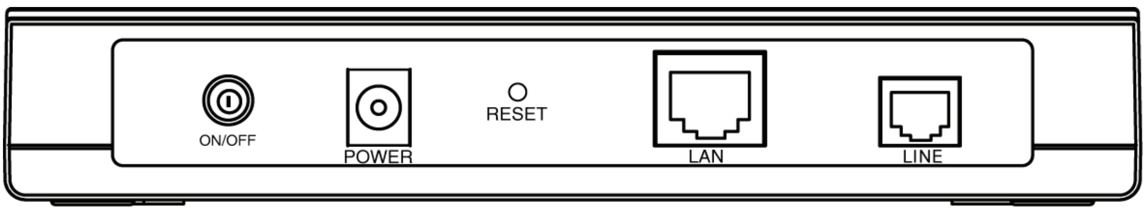


Figure 2-2

- ON/OFF: The switch for the power.
- POWER: The Power plug is where you will connect the power adapter.
- RESET: There are two ways to reset the Router's factory defaults.

  Method one: When the device is working, please press the reset button of the Router, keep the reset button pressed down for more than five seconds and then wait for the router to reboot.

  Method two: Restore the default setting from "Maintenance-SysRestart" of the Router's Web-based Utility.
- LAN: Through the port, you can connect the Router to your PC or the other Ethernet network

devices.

- LINE: Through the port, you can connect the Router with the telephone.

2.3 Installation Environment

- The Product should not be located where it will be exposed to moisture or excessive heat.
- Place the Router in a location where it can be connected to the various devices as well as to a power source.
- Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard.
- The Router can be placed on a shelf or desktop.

2.4 Connecting the Router

Before installing the device, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact your ISP. You need to connect the device to the phone jack, the power outlet, and your computer or network. Before cable connection, cut off the power supply and keep your hands dry. You can follow the steps below to install it.

Step 1: Connect the ADSL Line.

Method one: Plug one end of the twisted-pair ADSL cable into the ADSL LINE port on the rear panel of TD-8816B, and insert the other end into the wall socket.

Method two：You can use a separate splitter. External splitter can divide the data and voice, and then you can access the Internet and make calls at the same time. The external splitter has three ports:

- LINE: Connect to the wall jack
- PHONE: Connect to the phone sets
- MODEM: Connect to the ADSL LINE port of TD-8816B

Plug one end of the twisted-pair ADSL cable into the ADSL LINE port on the rear panel of TD-8816B. Connect the other end to the MODEM port of the external splitter.

Step 2: Connect the Ethernet cable. Attach one end of a network cable to your computer's Ethernet port or a regular hub/switch port, and the other end to the LAN port on the TD-8816B.

Step 3: Attach the power adapter. Connect the AC power adapter to the POWER connector on the rear of the device and plug in the adapter to a wall outlet or power extension.

Step 4: Turn on the TD-8816B and power on the computers and LAN devices.

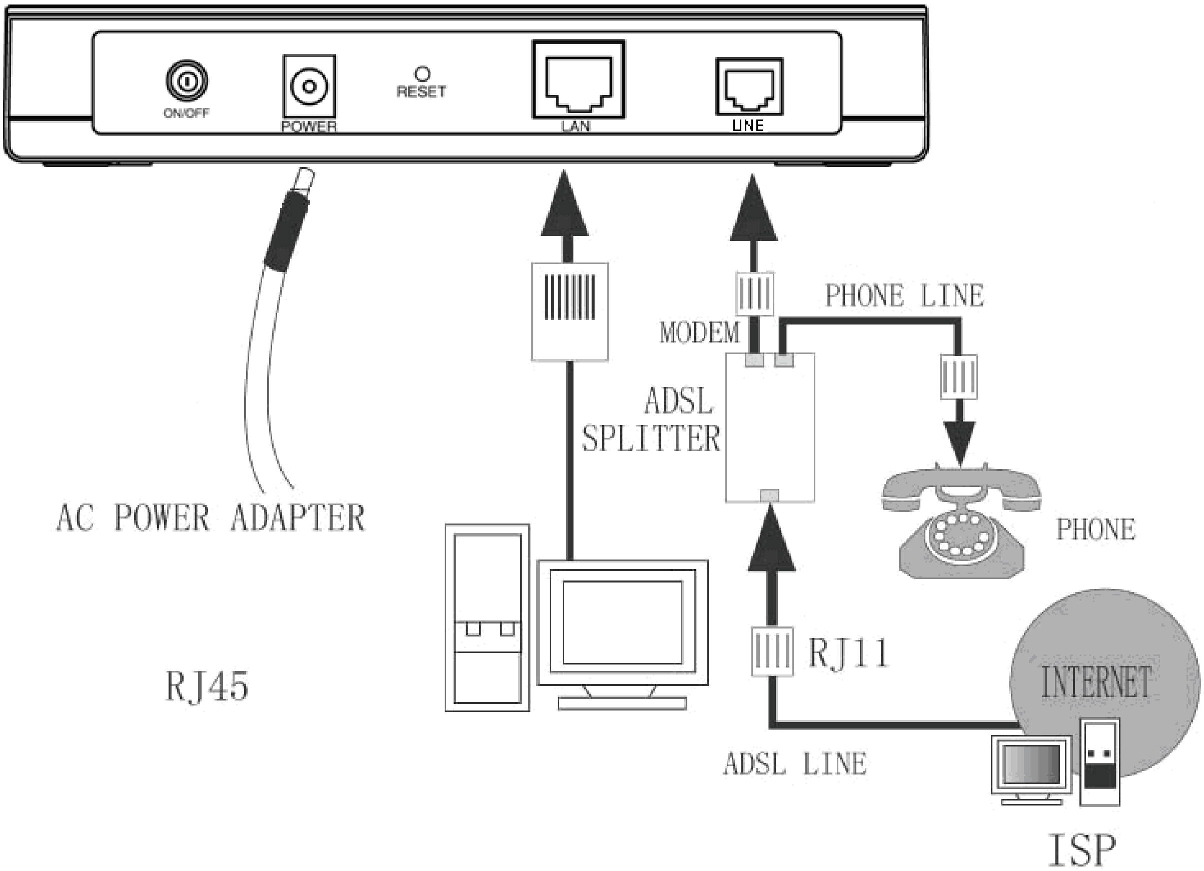

ON/OFF
POWER
RESET
LAN
LINE
PHONE LINE
MODEM
ADSL
SPLITTER
AC POWER ADAPTER
PHONE
RJ45
RJ11
INTERNET
ADSL LINE
ISP

Figure 2-3

Chapter 3. Quick Installation Guide

3.1 Configure PC

After you directly connect your PC to the TD-8816B or connect your adapter to a Hub/Switch which has connected to the Router, you need to configure your PC's IP address. Follow the steps below to configure it.

Step 1: Click the **Start** menu on your desktop, right click **My Network Places**, and then select **Properties** (shown in Figure 3-1).

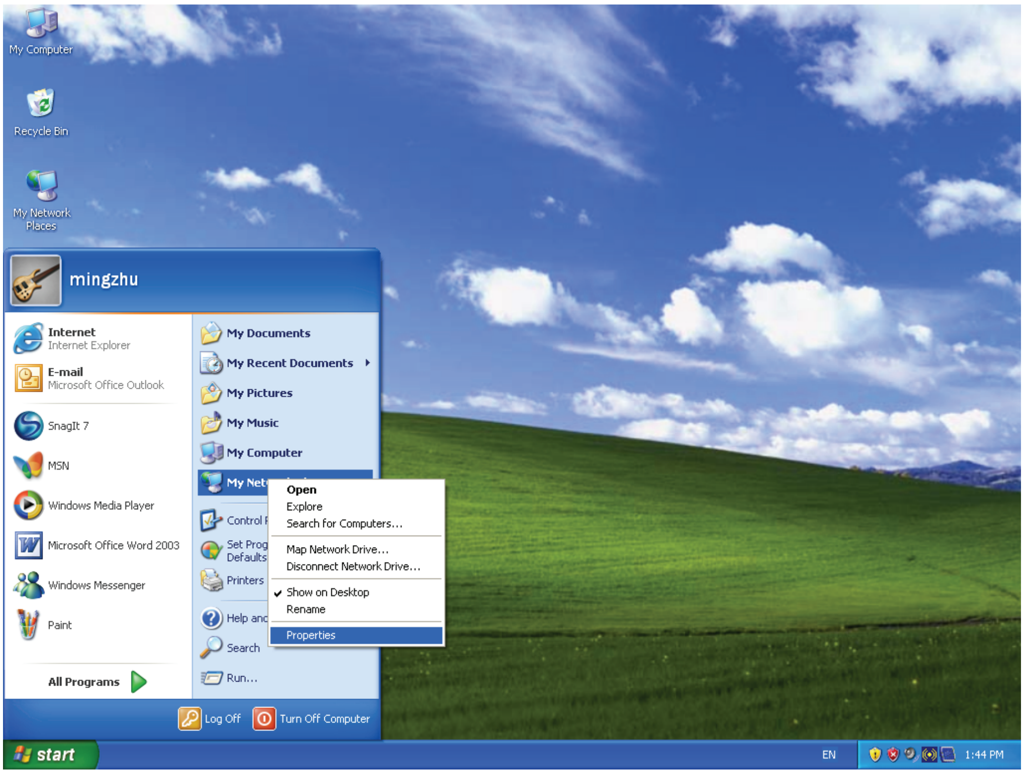


Figure 3-1

Step 2: Right click **Local Area Connection** (LAN), and then select **Properties**.

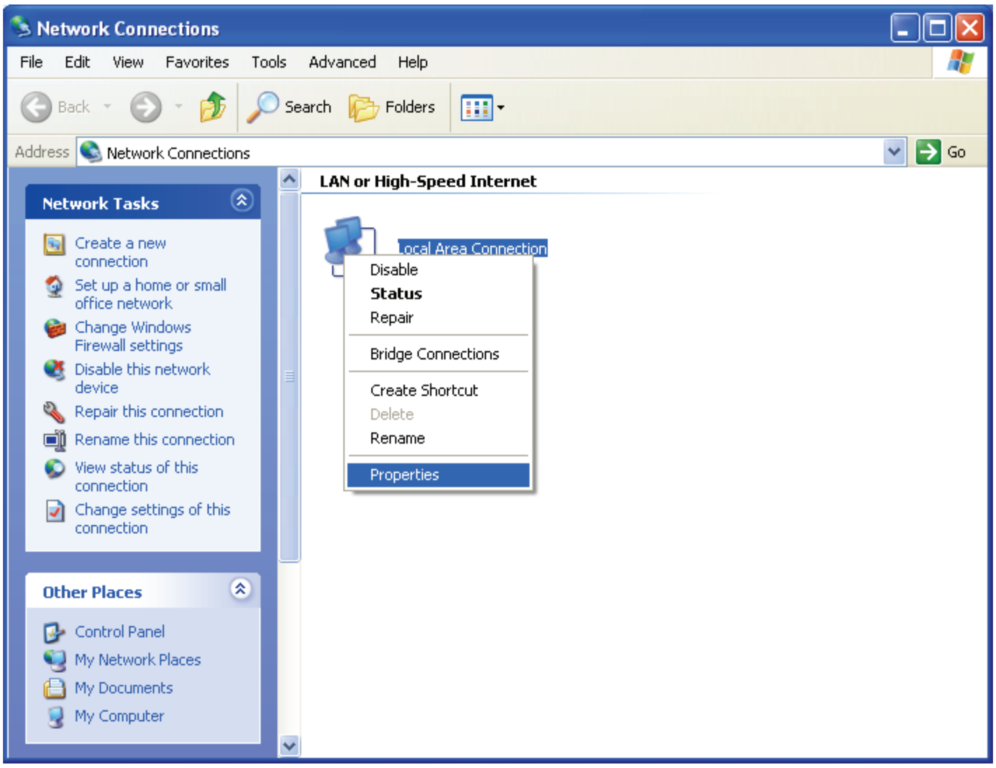


Figure 3-2

Step 3: Select **General** tab, highlight Internet Protocol (TCP/IP), and then click the **Properties** button.

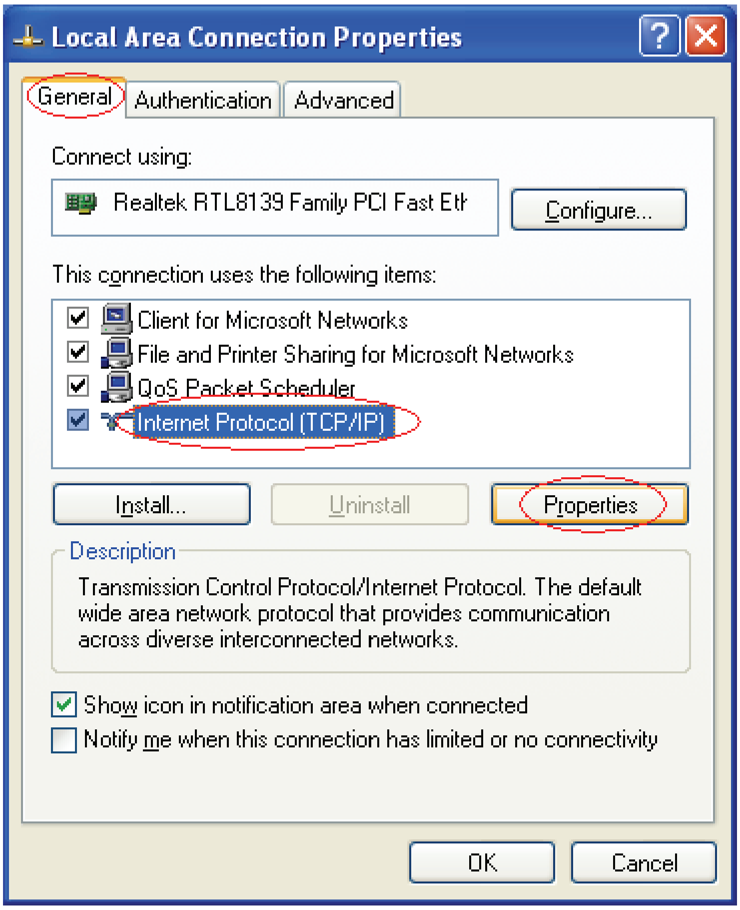


Figure 3-3

Step 4: Configure the IP address as Figure 3-4 shows. After that, click **OK**.

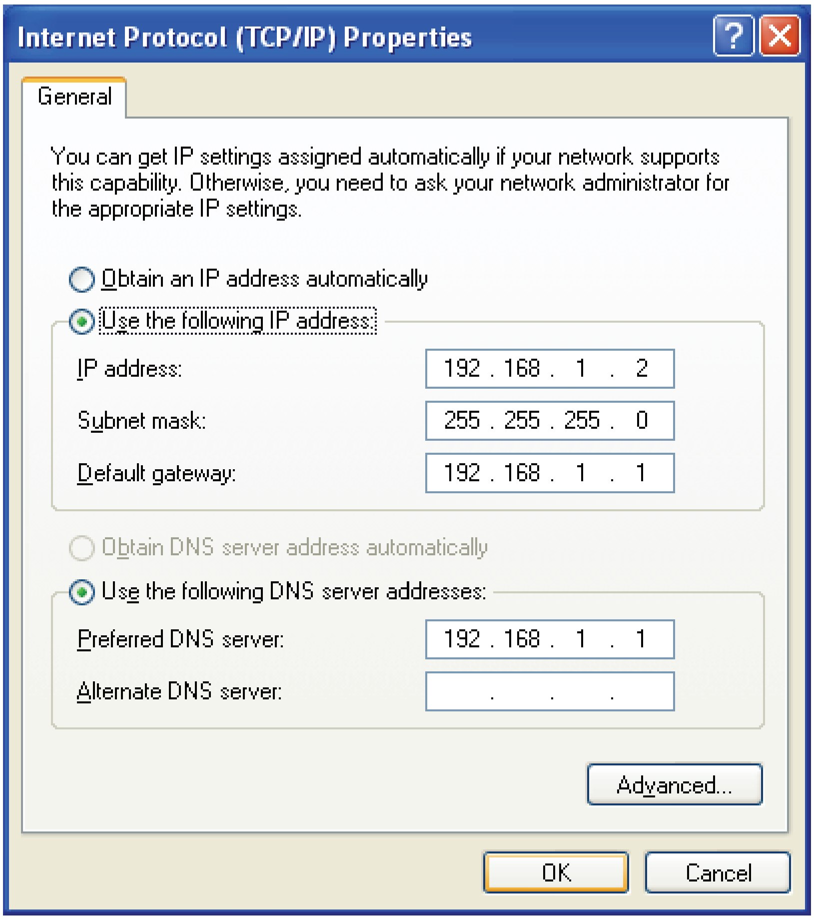


Figure 3-4

☞ **Note:**

You can configure the PC to get an IP address automatically, select "Obtain an IP address automatically" and "Obtain DNS server address automatically" in the screen above.

Now, you can run the Ping command in the command prompt to verify the network connection. Please click the **Start** menu on your desktop, select **run** tab, type **cmd** in the field, and then type *ping 192.168.1.1* on the next screen, and then press **Enter**.

If the result displayed is similar to the screen below, the connection between your PC and the Router has been established.

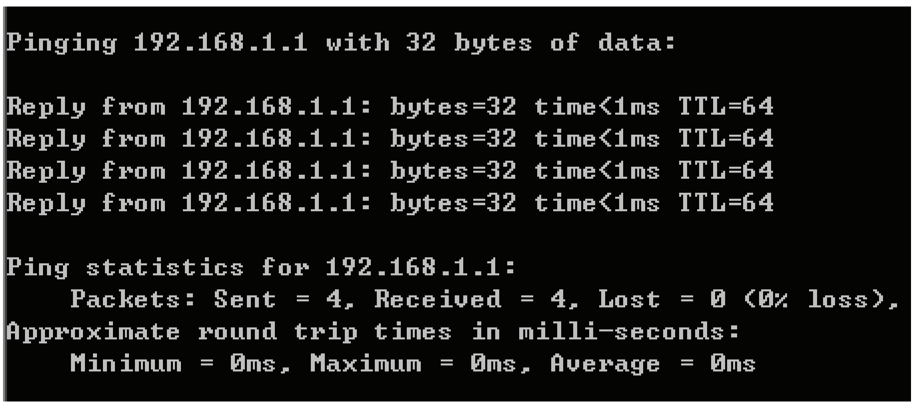


Figure 3-5

If the result displayed is similar to the screen shown below, it means that your PC has not connected to the Router.

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

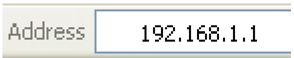
Figure 3-6

You can check it follow the steps below:

1) **Is the connection between your PC and the Router correct?**
   The LEDs of LAN port which you link to the device and the LEDs on your PC's adapter should be lit.
2) **Is the TCP/IP configuration for your PC correct?**
   If the Router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254.

3.2 Login

Once your host PC is properly configured, please proceed as follows to use the Web-based Utility: Start your web browser and type the private IP address of the Router in the URL field: **192.168.1.1**.



After that, you will see the screen shown below, enter the default User Name **admin** and the default Password **admin**, and then click **OK** to access to the **Quick Setup** screen. You can follow the steps below to complete the Quick Setup.



Figure 3-7

Step 1: Select the **Quick Start** tab, then click **RUN WIZARD**, and you will see the next screen. Click the **NEXT** button.

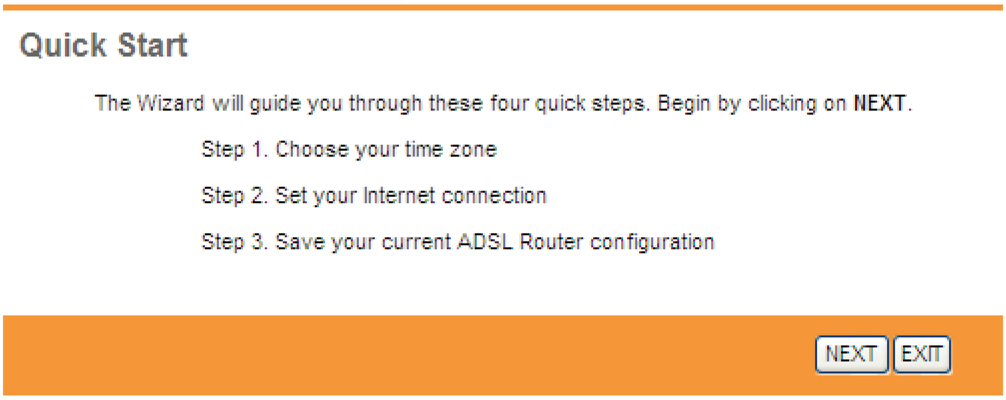


Figure 3-8

Step 2: Configure the time for the Router, and then click the **NEXT** button.

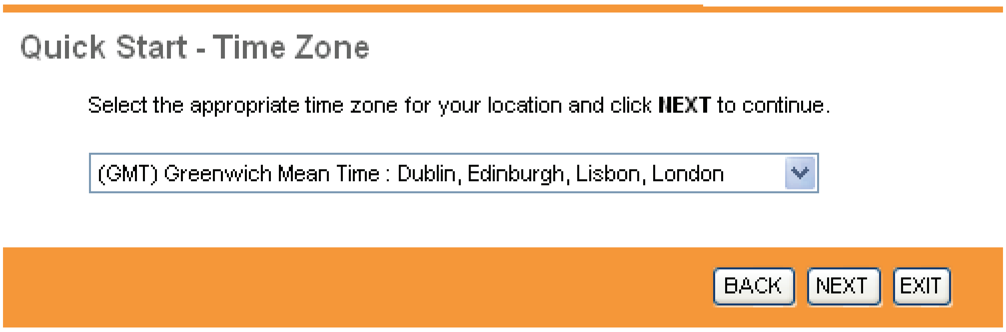


Figure 3-9

Step 3: Select the connection type to connect to the ISP (We select **PPPoE/PPPoA** mode for example here), and then click the **NEXT** button.

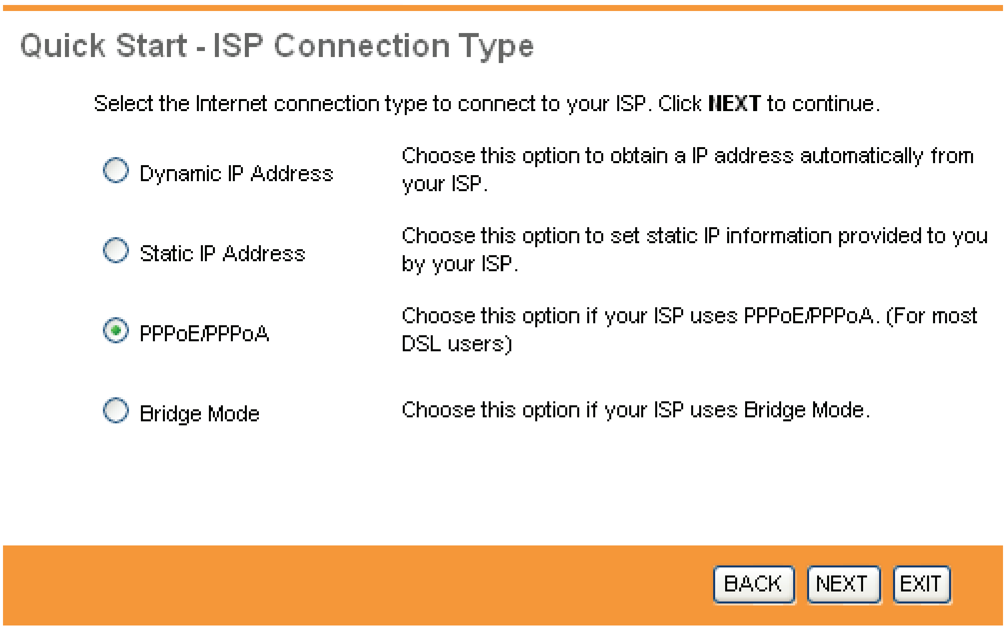


Figure 3-10

Step 4: Configure the following options provided by your ISP: **Username**, **Password**, **VPI**, **VCI** and **Connection Type**. Then click **Next**.

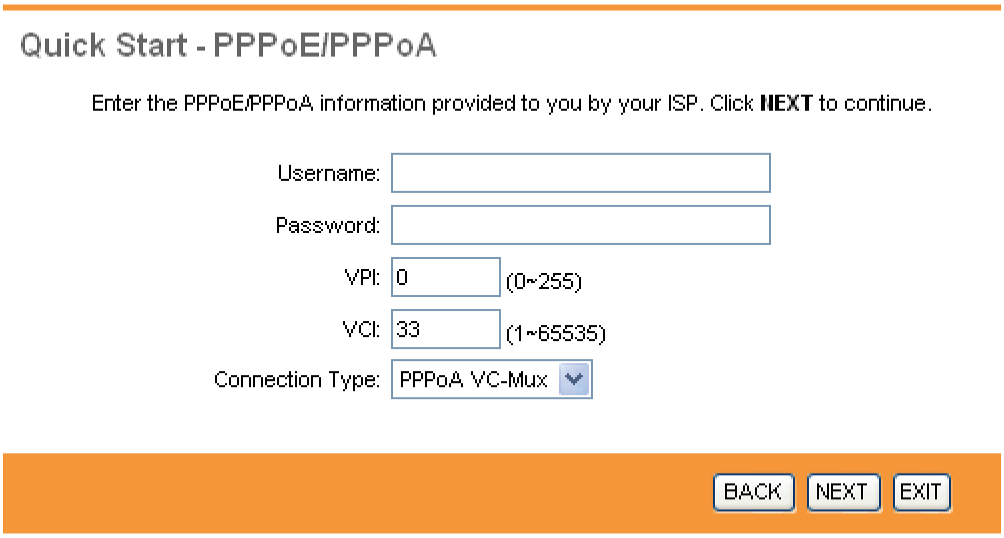


Figure 3-11

Step 5: Click **NEXT** to finish the Quick Start.

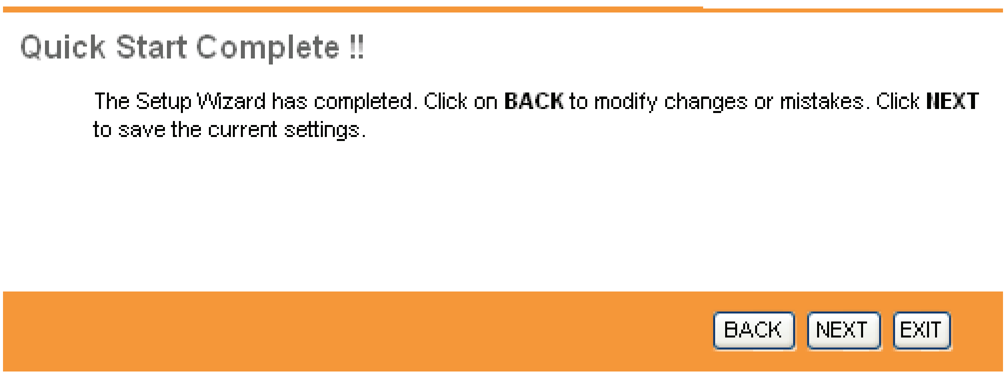


Figure 3-12

Chapter 4. Software Configuration

This User Guide recommends using the "Quick Installation Guide" for first-time installation. For advanced users, if you want to know more about this device and make use of its functions adequately, maybe you will get help from this chapter to configure the advanced settings through the Web-based Utility.

After your successful login, you can configure and manage the device. There are main menus on the top of the Web-based Utility, submenus will be available after you click one of the main menus. On the center of the Web-based Utility, there are the detailed configurations or status information. To apply any settings you have altered on the page, please click the **SAVE** button.

4.1 Status

Choose "**Status**", you can see the next submenus: **Device Info**, **System Log** and **Statistics**. Click any of them, and you will be able to configure the corresponding function.



Figure 4-1

Choose "**Status→Device Info**" menu, and you will be able to view the device information, including LAN, WAN and ADSL. The information will vary depending on the settings of the Router configured on the Interface Setup screen.

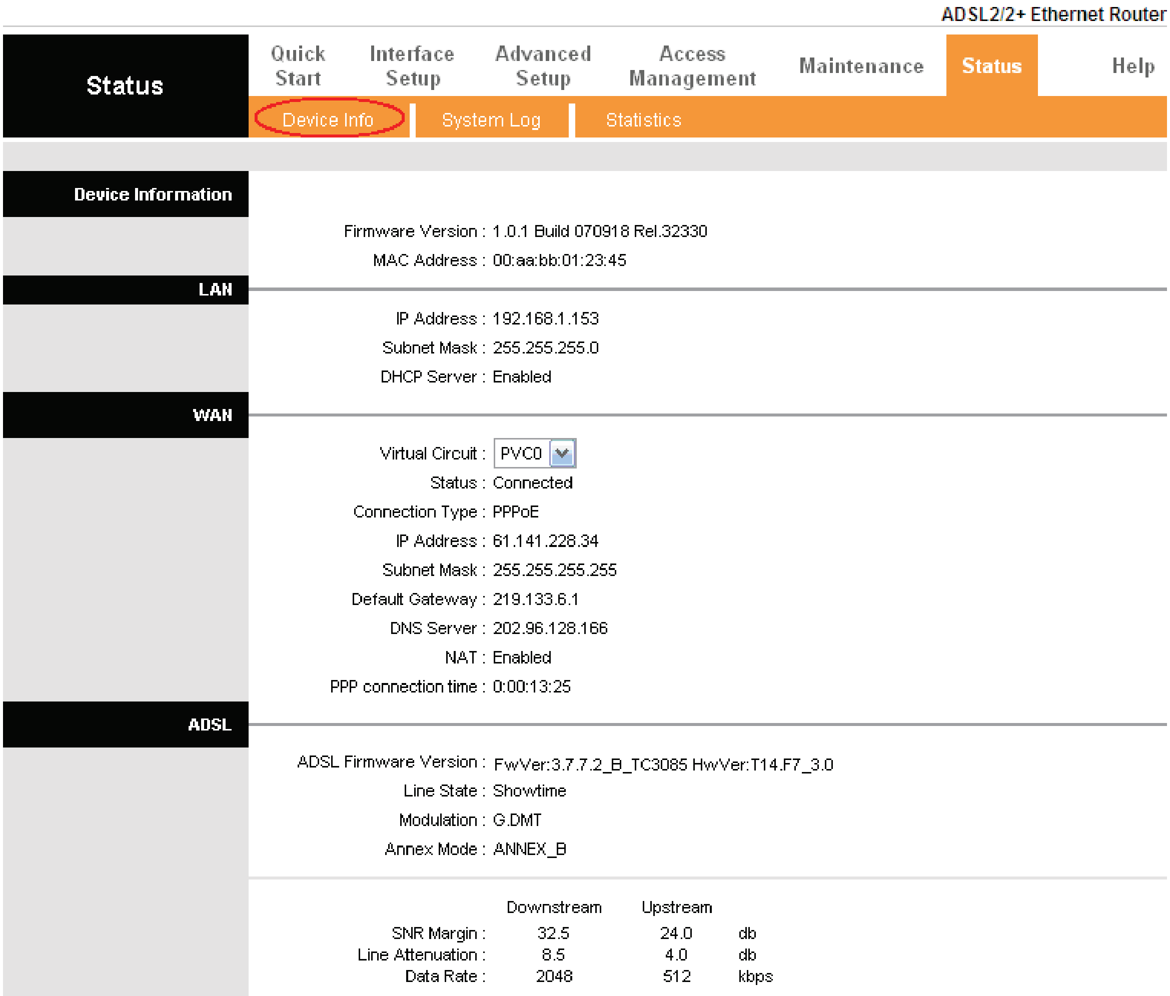


Figure 4-2

Note:

Click the other submenus **System Log** or **Statistics** in Figure 4-2, you will be able to view the system log and traffic statistics about the Router.

4.2 Quick Start

Please refer to " 3.2: Login".

4.3 Interface Setup

Choose "**Interface Setup**", you can see the next submenus: **Internet** and **LAN**.



Figure 4-3

Click any of them, and you will be able to configure the corresponding function.

4.3.1 Internet

Choose “**Interface Setup→Internet**” menu, you can configure the parameters for WAN ports in the next screen (shown in Figure 4-4).

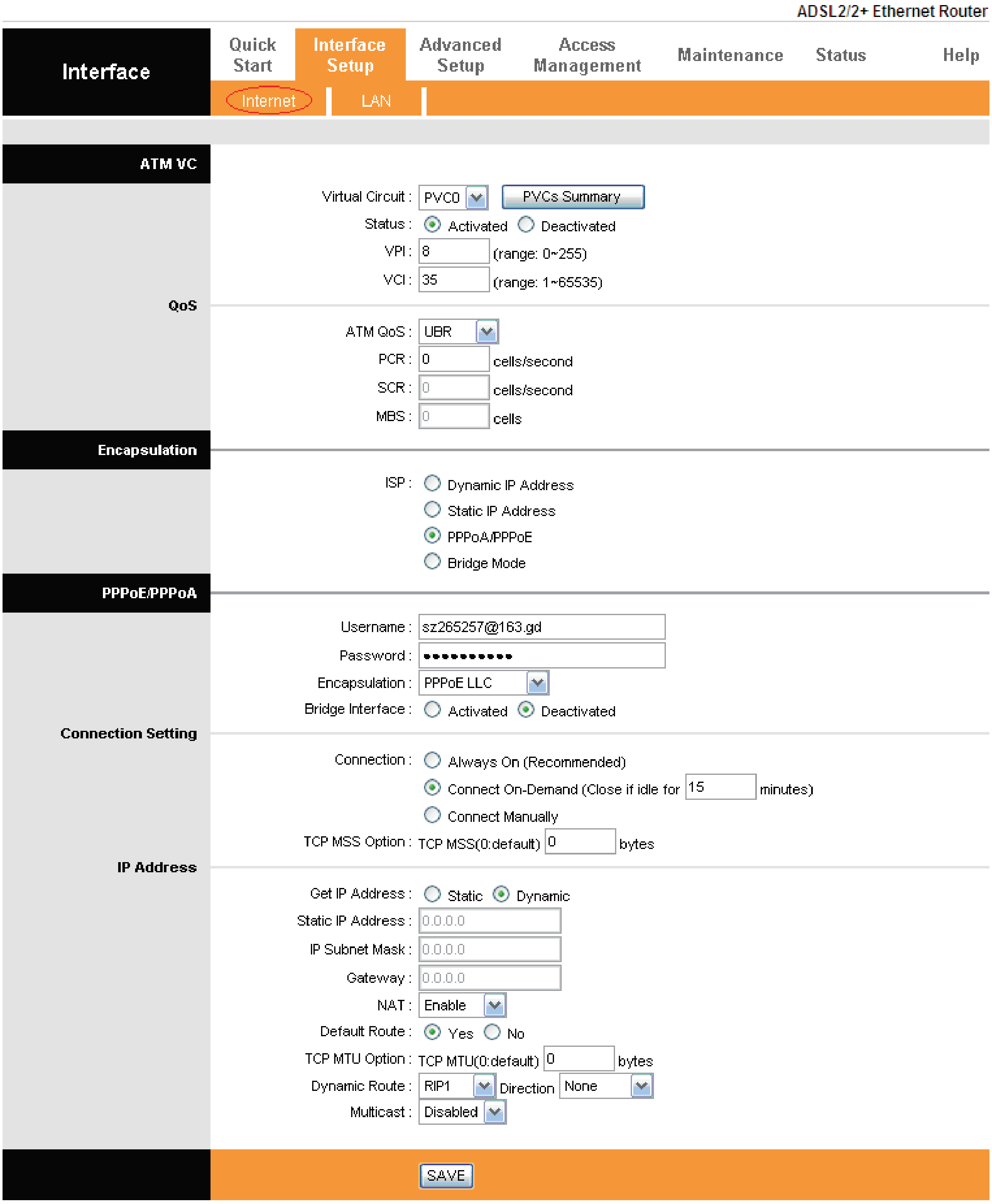


Figure 4-4

- **ATM VC:** ATM settings are used to connect to your ISP. Your ISP provides VPI (Virtual Path Identifier), VCI (Virtual Channel Identifier) settings to you. In this Device, you can totally setup 8 VCs on different encapsulations, if you apply 8 different virtual circuits from your ISP. You need to activate the VC to take effect. For PVCs management, you can use ATM QoS to setup each PVC traffic line's priority.

- **Virtual Circuit:** Select the VC number you want to setup, PVC0~PVC7.
- **Status:** If you want to use a designed VC, you should activate it.
- **VPI:** Identifies the virtual path between endpoints in an ATM network. The valid range is from 0 to 255. Please input the value provided by your ISP.
- **VCI:** Identifies the virtual channel endpoints in an ATM network. The valid range is from 32 to 65535 (1 to 31 is reserved for well-known protocols). Please input the value provided by your ISP.
- **PVCs Summary:** Click the button, you can view the summary information about the PVCs.
- **QoS:** Select the Quality of Service types for this Virtual Circuit, including CBR (Constant Bit Rate), UBR (Unspecified Bit Rate) and VBR (Variable Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR (Peak Cell Rate), SCR (Sustained Cell Rate) and MBS (Maximum Burst Size), please configure them according your needs.

➢ **Encapsulation:** There are four connection types: Dynamic IP Address, Static IP Address, PPPoA/PPPoE and Bridge Mode. Please choose the designed type that you want to use. After that, you should follow the configuration below to proceed.

1. Dynamic IP Address

Select this option if your ISP provides you an IP address automatically. This option is typically used for Cable services. Please enter the Dynamic IP information accordingly.

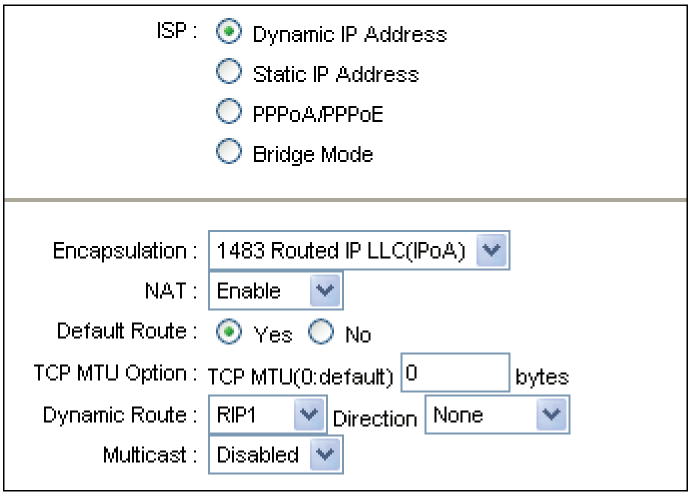


Figure 4-5

➢ **Encapsulation:** Select the encapsulation mode for the Dynamic IP Address, you can leave it default.

➢ **NAT:** Select this option to Enable/Disable the NAT (Network Address Translation) function for this VC. The NAT function can be activated or deactivated per PVC basis.

➢ **Default Route:** If enable this function, the current PVC will be considered as the default gateway to internet from this device.

➢ **TCP MTU Option:** Enter the TCP MTU as your desire.

➢ **Dynamic Route:** Select this option to specify the RIP (Routing Information protocol) version

for WAN interface, including **RIP1**, **RIP2-B** and **RIP2-M**. RIP2-B and RIP2-M are both sent in RIP2 format, the difference is that RIP2-M using Multicast, while RIP2-B using Broadcast format.

- **Direction:** Select this option to specify the RIP direction. **None** is for disabling the RIP function. **Both** means the ADSL Router will periodically send routing information and accept routing information, and then incorporate them into routing table. **IN only** means the ADLS router will only accept but will not send RIP packet. **OUT only** means the ADLS router will only send but will not accept RIP packet.

➢ **Multicast:** Select IGMP version, or disable the function. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The ADSL ATU-R supports both IGMP version 1 (**IGMP v1**) and **IGMP v2**. Select "Disabled" to disable it.

2. Static IP Address

Select this option if your ISP provides static IP information to you. You should set static IP address, IP subnet mask, and gateway address in the screen below (shown in Figure 4-6).

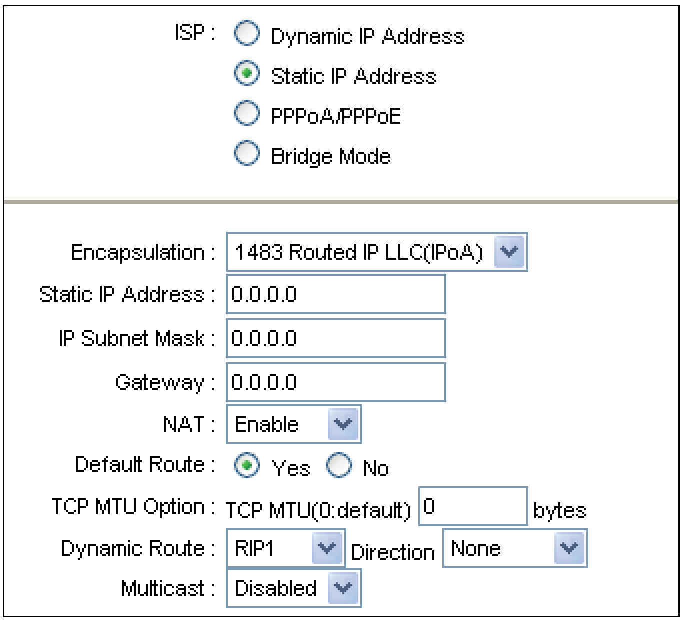


Figure 4-6

Note:

Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x), such as 192.168.1.100. The Router will not accept the IP address if it is not in this format.

3. PPPoA/PPPoE

Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL services. Select Dynamic PPPoE to obtain an IP address automatically for your PPPoE connection. Select Static PPPoE to use a static IP address for your PPPoE connection. Please enter the information accordingly.

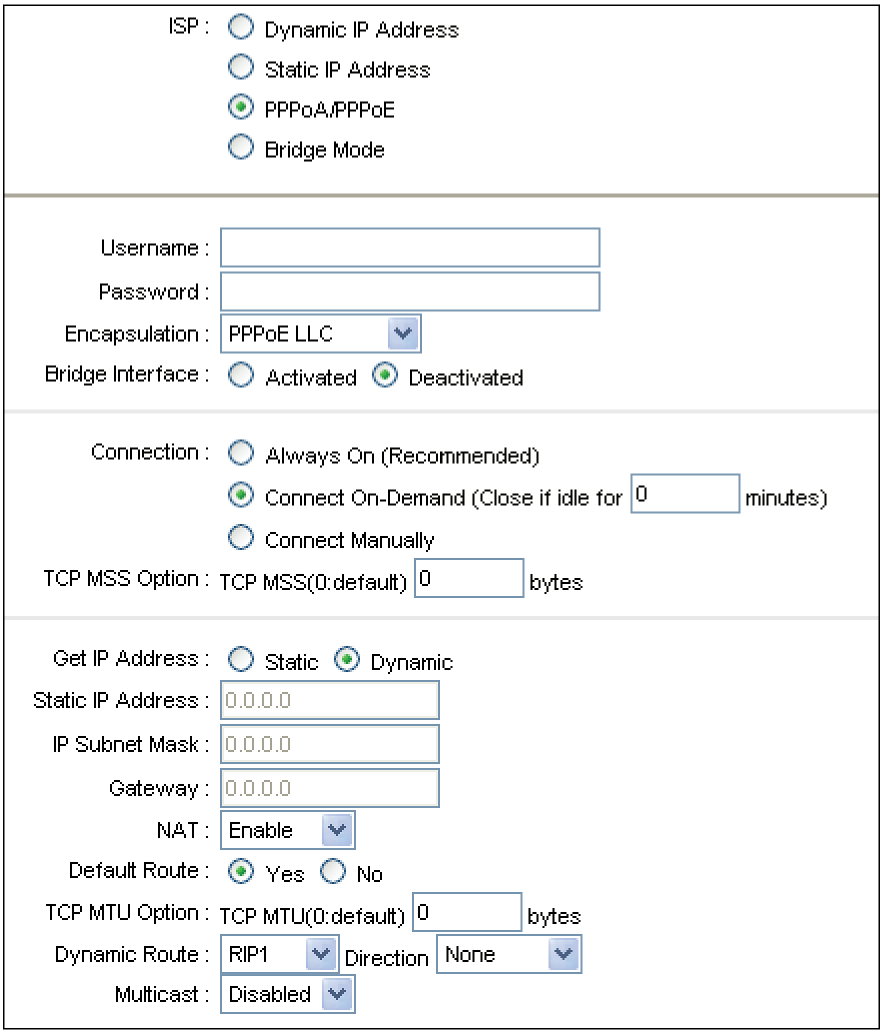


Figure 4-7

- **Username:** Enter your username for your PPPoE/PPPoA connection.
- **Password:** Enter your password for your PPPoE/PPPoA connection.
- **Encapsulation:** For both PPPoE/PPPoA connection, you need to specify the type of Multiplexing, either LLC or VC Mux.
- **Bridge Interface:** Activate the option, the Router can also work in Bridge mode.
- **Connection:** For PPPoE/PPPoA connection, you can select **Always on** or **Connect on-Demand** or **Connect Manually**. Connect on demand is dependent on the traffic. If there is no traffic (or **Idle**) for a pre-specified period of time), the connection will tear down automatically. And once there is traffic send or receive, the connection will be automatically on.
- **Static/Dynamic IP Address:** For PPPoE/PPPoA connection, you need to specify the public IP address for this ADSL Router. The IP address can be either dynamically (via DHCP) or given IP address provided by your ISP. For Static IP, you need to specify the IP address, Subnet Mask and Gateway IP address.
- **Default Route:** You should select **Yes** to configure the PVC as the default gateway to internet from this device.

4. Bridge Mode

If you select this type of connection, the modem can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN.

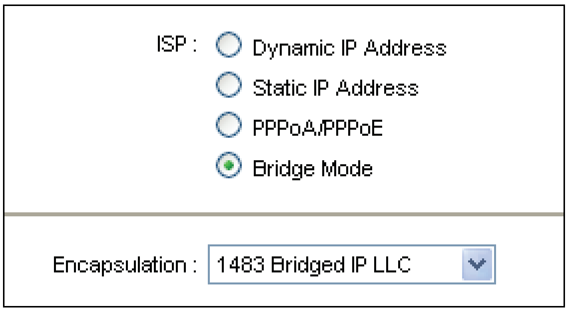


Figure 4-8

Note:

After you finish the Internet configuration, please click SAVE to make the settings take effect.

4.3.2 LAN

Choose "**Interface Setup→LAN**" menu, and you will see the LAN screen (shown in Figure 4-9). Please configure the parameters for LAN ports according to the descriptions below.

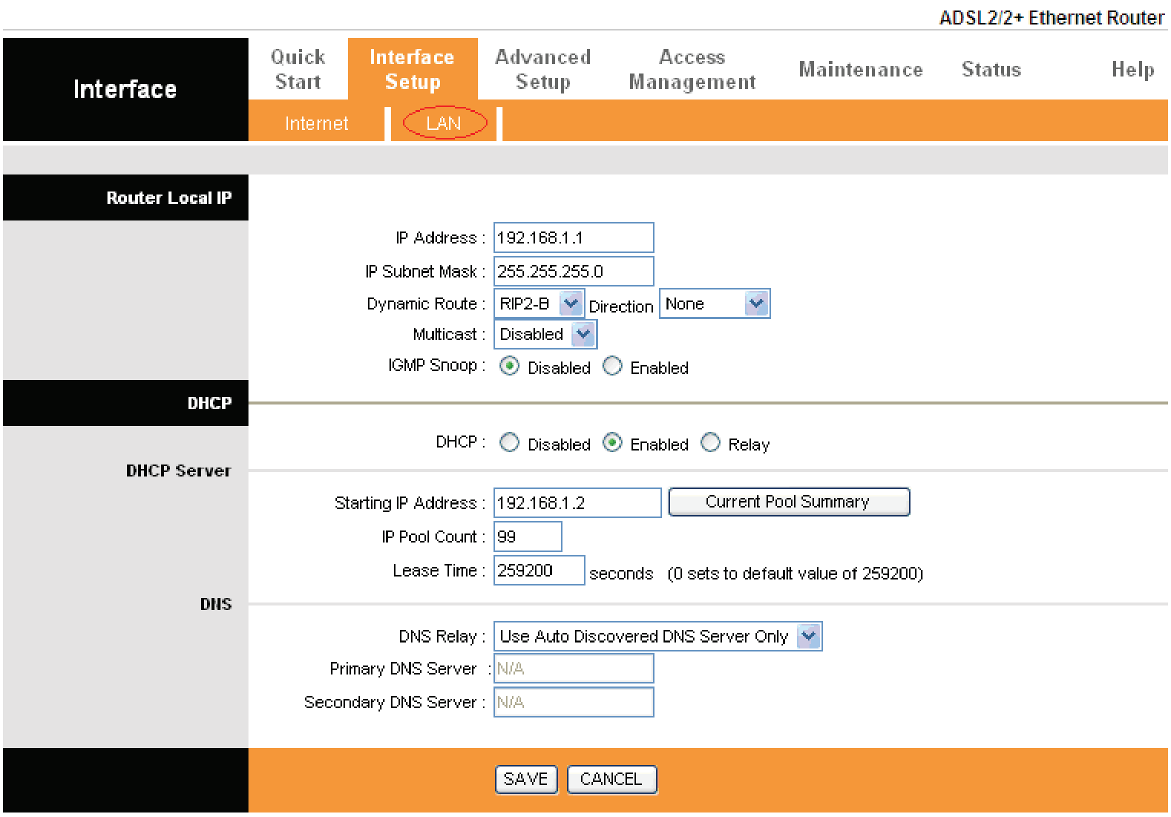


Figure 4-9

➢ **Router Local IP:** These are the IP settings of the LAN interface for the device. These settings may be referred to as Private settings. You may change the LAN IP address if

needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

- **IP Address:** Enter the Router's local IP Address, then you can access to the Web-based Utility via the IP Address, the default value is 192.168.1.1.
- **IP Subnet Mask:** Enter the Router's Subnet Mask, the default value is 255.255.255.0.
- **Dynamic Route:** Select this option to specify the RIP (Routing Information protocol) version for LAN interface, including **RIP1**, **RIP2-B** and **RIP2-M**. RIP2-B and RIP2-M are both sent in RIP2 format, the difference is that RIP2-M using Multicast, while RIP2-B using Broadcast format.
- **Direction:** Select this option to specify the RIP direction. **None** is for disabling the RIP function. **Both** means the ADSL Router will periodically send routing information and accept routing information, and then incorporate them into routing table. **IN only** means the ADLS router will only accept but will not send RIP packet. **OUT only** means the ADLS router will only send but will not accept RIP packet.
- **Multicast:** Select IGMP version, or disable the function. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The ADSL ATU-R supports both IGMP version 1 (**IGMP v1**) and **IGMP v2**. Select "Disabled" to disable it.
- **IGMP Snoop:** Enable the IGMP Snoop function if you need.

➢ **DHCP Server:** Select **Enabled**, then you will see the screen below (shown in Figure 4-10). The Router will work as a DHCP Server, it becomes the default gateway for DHCP client connected to it. DHCP stands for Dynamic Host Control Protocol. The DHCP Server gives out IP addresses when a device is booting up and request an IP address to be logged on to the network. That device must be set as a DHCP client to obtain the IP address automatically. By default, the DHCP Server is enabled. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.

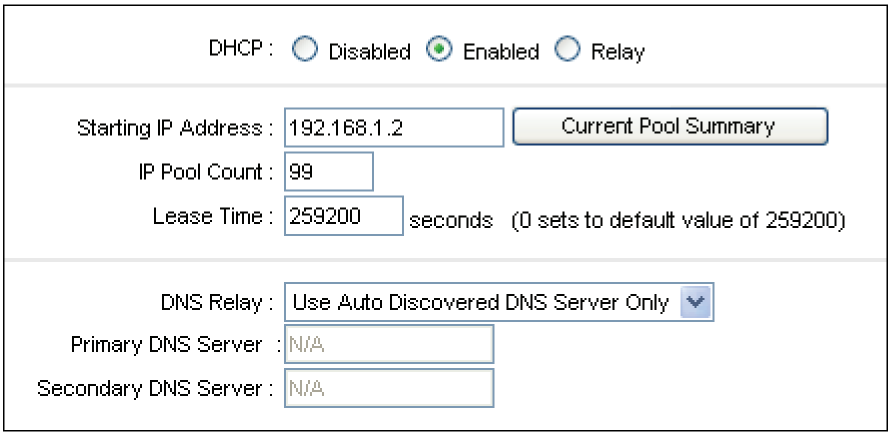


Figure 4-10

- **Starting IP Address:** Enter the starting IP address for the DHCP server's IP assignment. Because the default IP address for the Router is 192.168.1.1, the default Start IP Address is **192.168.1.2**, and the Start IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

- **IP Pool Count:** The max user pool size.
- **Lease Time:** The length of time for the IP lease. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **259200** seconds.
- **DNS Relay:** If you want to disable this feature, you just need to set both Primary and secondary DNS IP to 0.0.0.0. If you want to use DNS relay, you can setup DNS server IP to 192.168.1.1 on their Computer. If not, the device will perform as no DNS relay.
- **Primary DNS Server:** Type in your preferred DNS server.
- **Secondary DNS Server:** Type in your preferred DNS server.
- **Current Pool Summary:** Click the button, you can view the IP addresses that the DHCP Server gives out.

☞ **Note:**

If **Use Auto Discovered DNS Server Only** is selected in DNS Relay, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If **Use User Discovered DNS Server Only** is selected in DNS Relay, it is necessary for you to enter the primary and optional secondary DNS server IP addresses. After type in the address, click SAVE button to save it and invoke it.

➢ **DHCP Relay:** Select **Relay**, then you will see the next screen (shown in Figure 4-11), the Router will work as a DHCP Relay. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.

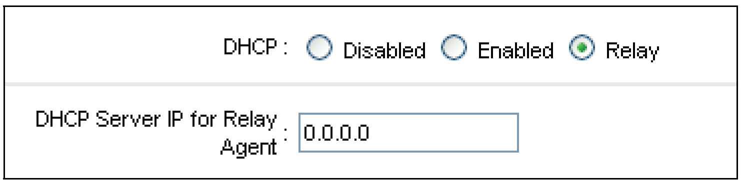


Figure 4-11

- **DHCP Server IP for Relay Agent:** Enter the DHCP server IP Address runs on WAN side.

☞ **Note:**

If you select **Disabled**, the DHCP function will not take effect.

4.4 Advanced Setup

Choose "**Advanced Setup**", you can see the next submenus:



Figure 4-12

Click any of them, and you will be able to configure the corresponding function.

4.4.1 Firewall

Choose "**Advanced Setup→Firewall**" menu, and you will see the next screen (shown in Figure 4-13).

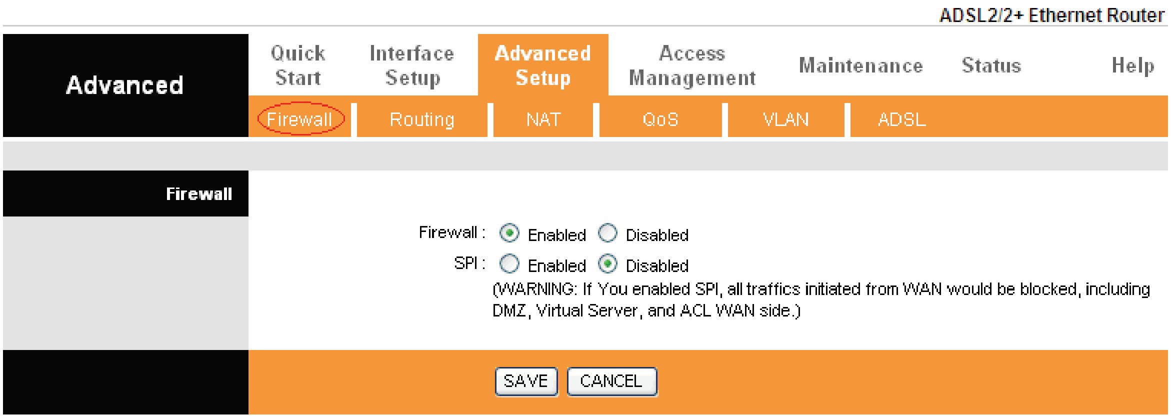


Figure 4-13

- **Firewall:** Select this option can automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.
- **SPI:** If you enable SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

4.4.2 Routing

Choose "**Advanced Setup→Routing**" menu, and you will see the routing information in the next screen (shown in Figure 4-14).

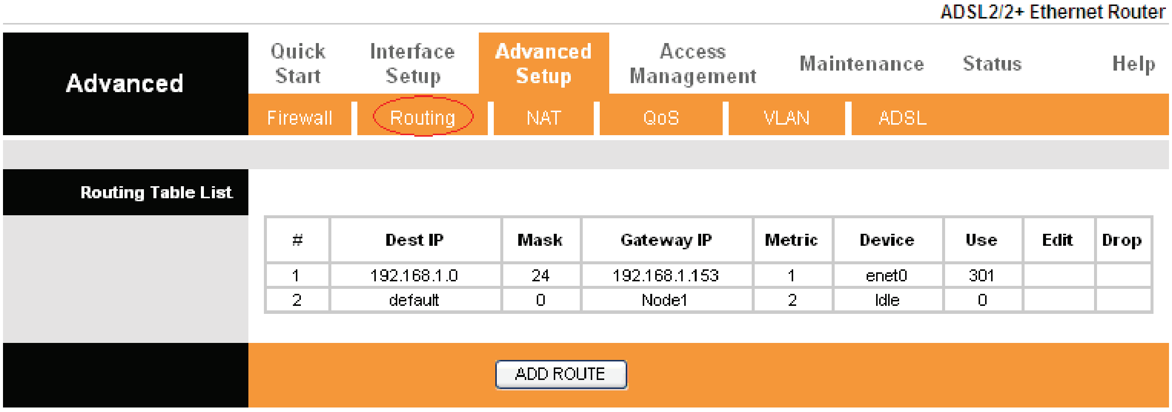


Figure 4-14

Click **ADD ROUTE** button to add a new route in the next screen (shown in Figure 4-15).

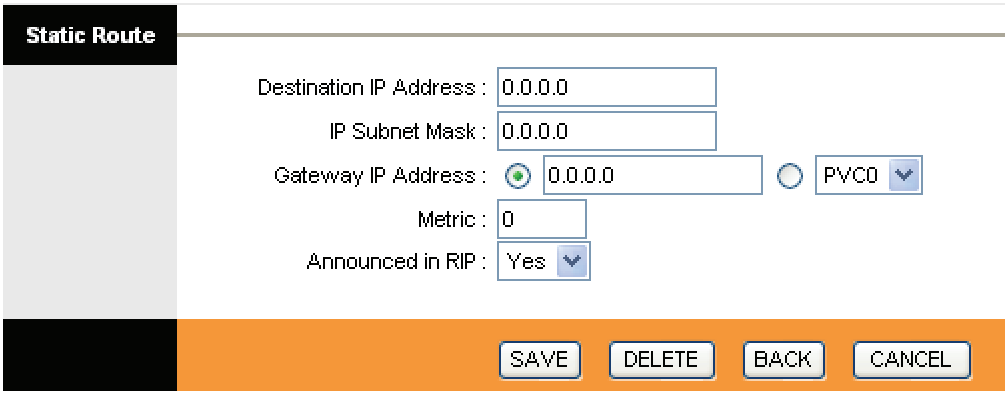


Figure 4-15

- **Destination IP Address:** This parameter specifies the IP network address of the final destination.
- **IP Subnet Mask:** Enter the subnet mask for this destination.
- **Gateway IP Address:** Enter the IP address of the gateway. The gateway is an immediate neighbor of your ADSL Router that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Router; over Internet (WAN), the gateway must be the IP address of one of the remote nodes.
- **Metric:** Metric represents the "cost" of transmission for routing purposes. IP Routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not to be precise, but it must between 1 and 15. In practice, 2 or 3 is usually a good number.
- **Announced in RIP:** This parameter determines if the ADSL router will include the route to this remote node in its RIP broadcasts. If set to Yes, the route to this remote node will be propagated to other hosts through RIP broadcasts. If No, this route is kept private and is not included in RIP broadcasts.

4.4.3 NAT

Choose “**Advanced Setup→NAT**” menu, you can setup the NAT (Network Address Translation) function for the Router (shown in Figure 4-16).

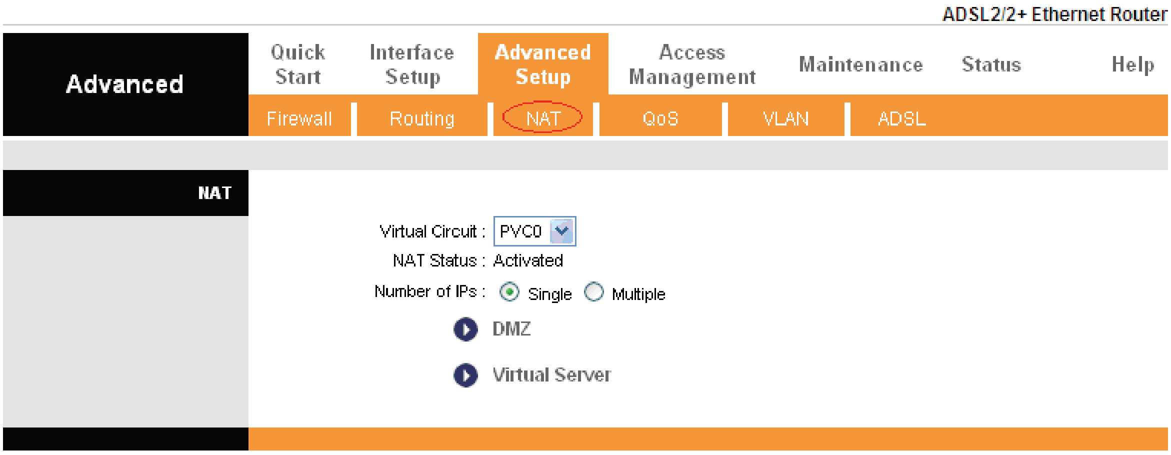


Figure 4-16

- **Virtual Circuit:** Enter Virtual Circuit Index that you plan to setup for the NAT function.
- **NAT Status:** This field shows the current status of the NAT function for the current VC. You can go to the previous screen (shown in Figure 4-4) to activate the function.
- **Number of IPs;** This field is to specify how many IPs are provided by your ISP for current VC. It can be single IP or multiple IPs. We select Multiple to explain.

Note:

For VCs with single IP, they share the same DMZ and Virtual servers; for VCs with multiple IPs, each VC can set DMZ and Virtual servers. Furthermore, for VCs with multiple IPs, they can define the Address Mapping rules; for VCs with single IP, since they have only one IP, there is no need to individually define the Address Mapping rule.

4.4.3.1. DMZ

Choose "**Advanced Setup→NAT→DMZ**" in Figure 4-16, you can configure the DMZ host in the next screen. A DMZ (demilitarized zone) is a host between a private local network and the outside public network. It prevents outside users from getting direct access to a server that has company data. Users of the public network outside the company can access to the DMZ host.

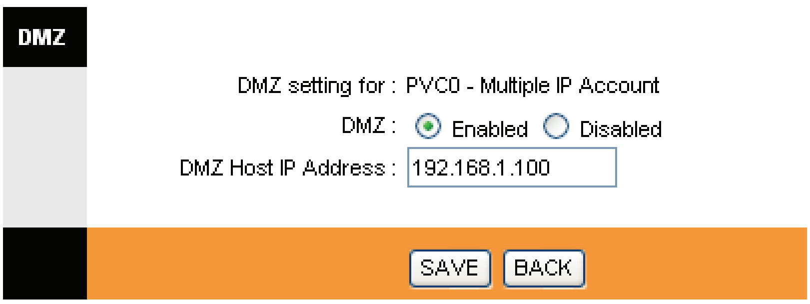


Figure 4-17

- **DMZ Host IP Address:** Enter the specified IP Address for DMZ host on the LAN side.

4.4.3.2. Virtual Server

Choose "**Advanced Setup→NAT→Virtual Server**" in Figure 4-16, you can configure the Virtual Server in the next screen.

The Virtual Server is the server or server(s) behind NAT (on the LAN), for example, Web server or FTP server, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

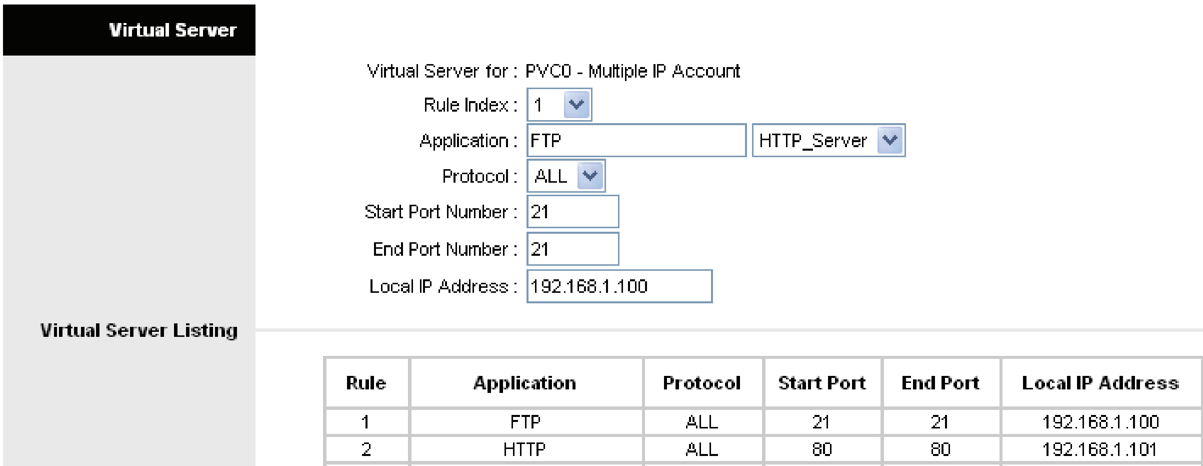


Figure 4-18

- **Rule Index:** The Virtual server rule index for this VC. You can specify 10 rules in maximum. All the VCs with single IP will use the same Virtual Server rules.
- **Start & End port number:** Enter the specific Start and End Port number you want to forward. If it is one port only, you can enter the End port number the same as Start port number. For example, you want to set the FTP Virtual server, you can set the start and end port number to 21.
- **Local IP Address:** Enter the IP Address for the Virtual Server in LAN side.
- **Virtual Server Listing:** This displays the information about the Virtual Servers you establish.

To add a virtual server entry:

Step 1: Select the "Virtual Circuit" and select "Number of IPs". After that, select the tab **IP Address Mapping** for the Virtual server (shown in Figure 4-16).

☞ **Note:**

For VCs with single IP, select **Single**; For VCs with multiple IPs, select **Multiple** for the option.

Step 2: Select the Rule index for the rule as shown in Figure 4-18.

Step 3: Select the application you want from drop-down list, then the protocol and port number will be added to the corresponding field automatically, you only need to configure the IP address for the virtual server; If the application list does not contain the service that you want, please configure the Port number, IP Address and Protocol manually.

Step 4: After that, click **SAVE** to make the entry take effect.

Other configurations for the entries as shown in Figure 4-18:

Enter the index of assigned entry, click the **DELETE** button to delete the entry.

Click the **Back** button to return to the previous screen.

Click the **CANCEL** button to cancel the configuration which is made just now.

4.4.3.3. IP Address Mapping

Choose "**Advanced Setup→NAT→IP Address Mapping**" in Figure 4-16, you can configure the Address Mapping Rule in the next screen. The IP Address Mapping is for those VCs that configured with multiple IPs. The IP Address Mapping rule is per-VC based (only for Multiple IPs' VCs).

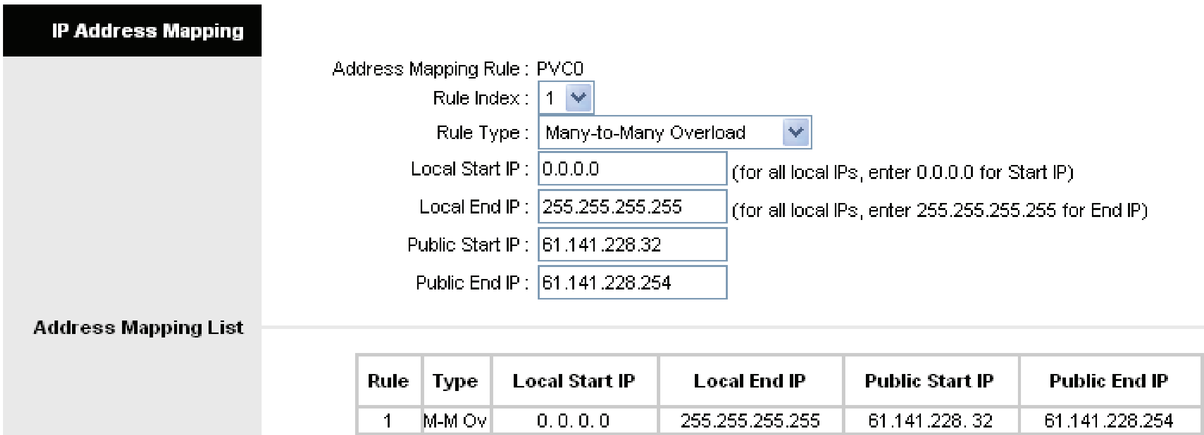


Figure 4-19

- **Rule Index:** Select the Virtual server rule index for this VC. You can specify 10 rules in maximum. All the VCs with single IP will use the same Virtual Server rules.
- **Rule Type:** There are four types of one-to-one, Many-to-One, Many-to-Many Overload and Many-to-Many No-overload.
- **Local Start & End IP:** Enter the local IP Address you plan to mapped to. Local Start IP is the starting local IP address and Local End IP is the ending local IP address. If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.
- **Public Start & End IP:** Enter the public IP Address you want to do NAT. Public Start IP is the starting public IP address and Public End IP is the ending public IP address. If you have a dynamic IP, enter 0.0.0.0 as the Public Start IP.
- **Address Mapping List:** This displays the information about the Mapping addresses.

To add a mapping rule:

Step 1: Select the "Virtual Circuit" and Multiple for the "Number of IPs". Then select the tab **IP Address Mapping** for the Virtual server (shown in Figure 4-16)..

☞ **Note:**

IP Address Mapping is only available for VCs with Multiple IPs.

Step 2: Select the Rule index for the rule as shown in Figure 4-19.

Step 3: Select the rule type you want from the drop-down list.

Step 4: Enter the local and public IP addresses in the corresponding fields.

Step 5: After that, click **SAVE** to make the entry take effect.

Other configurations for the entries as shown in Figure 4-19:

Enter the index of assigned entry, click the **DELETE** button to delete the entry.

Click the **Back** button to return to the previous screen.

Click the **CANCEL** button to cancel the configuration which is made just now.

4.4.4 QoS

Choose "**Advanced Setup→QoS**", you can configure the QoS in the next screen. QoS helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based priority. This is useful when there are certain types of data you want to give higher priority, such as voice data packets give higher priority than Web data packets. This option will provide better service of selected network traffic over various technologies.

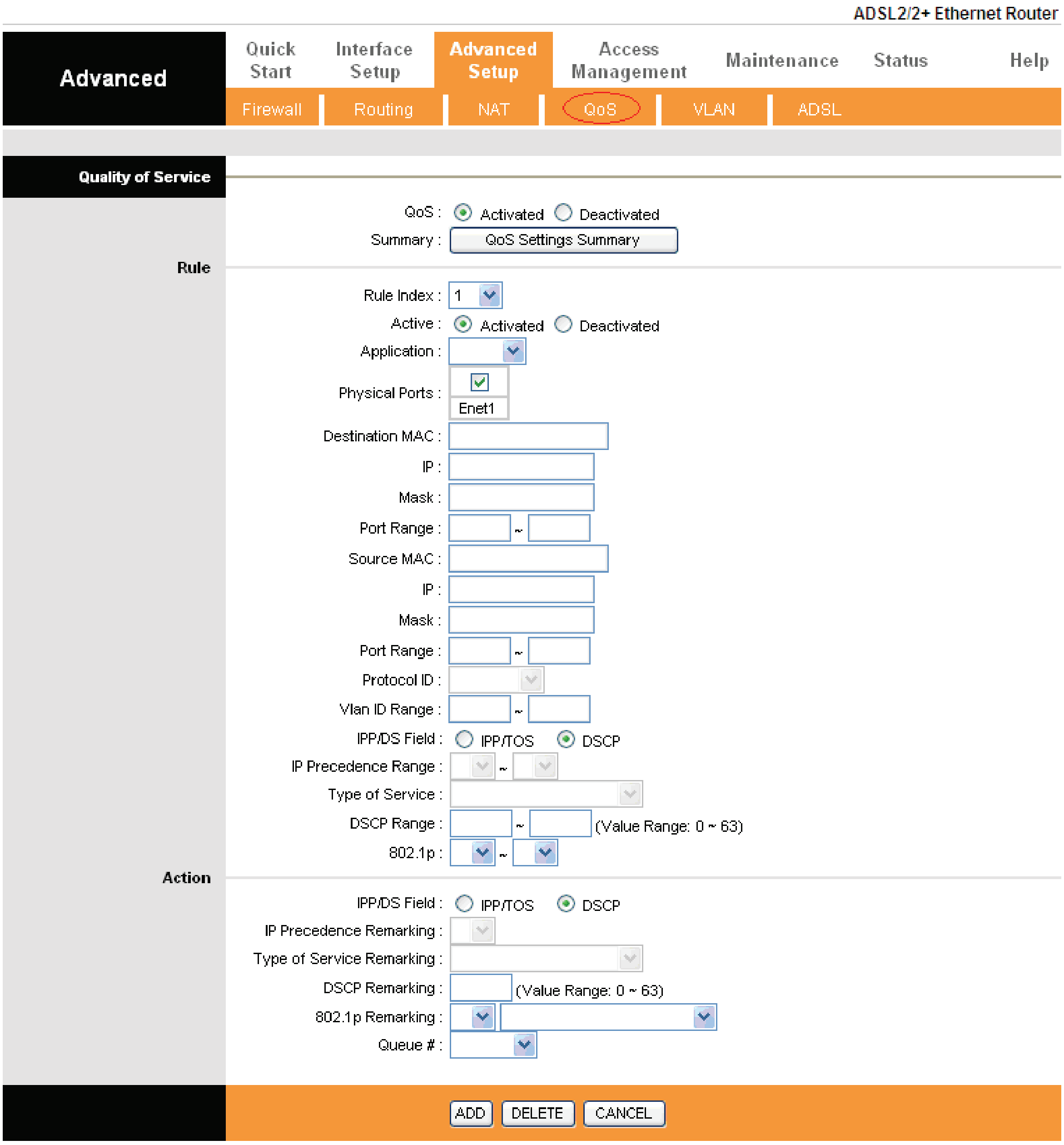


Figure 4-20

➢ **QoS:** Select this option to Activated/Deactivated the IP QoS on different types (IP ToS and

DiffServ).

- **Summary:** Click the button to view the configurations of QoS.
- **Rule:** Configure the rules for QoS. If the traffic complies with the rule, then the Router will take the corresponding action to deal with it.
  - **Rule Index:** Select the index for the rule you want to configure.
  - **Active:** Activate the rule. The rule can take effect only when it is activated.
  - **Application:** Select the application that the rule aimed at.
  - **Physical Ports:** Select the port whose traffic flow are controlled by the rule.
  - **Destination MAC & IP & Mask & Port Range:** Enter the IP information about the Destination host for the rule.
  - **Source MAC & IP & Mask & Port Range:** Enter the IP information about the Source host for the rule.
  - **Protocol ID:** Select one among TCP/UDP, TCP, UDP or ICMP protocols for the application.
  - **VLAN ID Range:** Enter the VLAN range, then the rule will be effective to the selected VLANs.
  - **IPP/DS Field:** Select the type of the action to assign the priority.

When you select IPP/TOS, you can assign the priority via IP information. IP QoS function is intended to deliver guaranteed as well as differentiated Internet services by giving network resource and usage control to the Network operator.

- **IP Precedence Range:** Enter the IP precedence range that the Router takes to differentiate the traffic.
- **Type of Service:** Select the type of service that the Router takes to deal with the traffic.
- **802.1p:** Select the priority range for the rule.

When you select DSCP, you can assign the priority via DHCP (the header of IP group). It maps the IP group into corresponding service class.

- **DSCP Range:** Enter the DSCP range to differentiate the traffic.
- **802.1p:** Select the priority range for the rule.

- **Action:** Configure the action that the Router takes to deal with the traffic which accord with the rule.
  - **IPP/DS Field:** Select the type for the action.
  - **IP Precedence Remarking:** Select the number to remark the priority for IP precedence.
  - **Type of Service Remarking:** Select the type to remark the service.
  - **DSCP Remarking:** Enter the number to remark the DSCP priority.
  - **802.1p Remarking:** Select the type to remark the 802.1p priority.
  - **Queue:** Select the priority type for the action.

4.4.5 VLAN

Choose "**Advanced Setup→VLAN**", you can activate the VLAN function in the next screen.

Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured so that they

can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization. There are two types of VLAN as follows:

Port-Based VLAN: Each physical switch port is configured with an access list specifying membership in a set of VLANs.

ATM VLAN: Using LAN Emulation (LANE) protocol to map Ethernet packets into ATM cells and deliver them to their destination by converting an Ethernet MAC address into an ATM address.

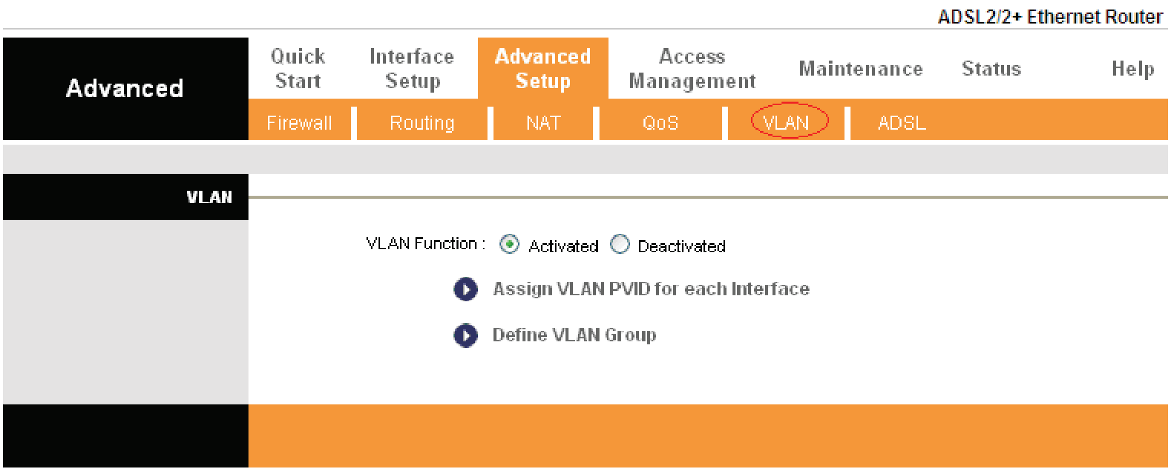


Figure 4-21

1. Assign VLAN PVID for each Interface

Click **Assign VLAN PVID for each Interface** in Figure 4-21, you can assign the PVID for each interface in the next screen (shown in Figure 4-22).

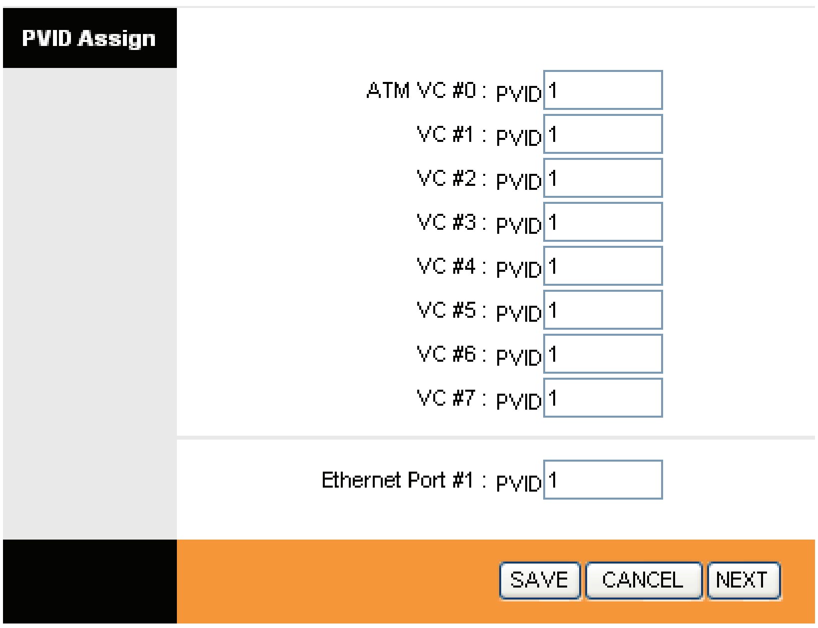


Figure 4-22

- **PVID:** Each physical port has a default VID called PVID (Port VID). PVID is assigned to untagged frames or priority tagged frames (frames with null (0) VID) received on this port.

2. Define VLAN Group

Click **Define VLAN Group** in Figure 4-21, you can define VLAN groups in the next screen (shown in Figure 4-23).

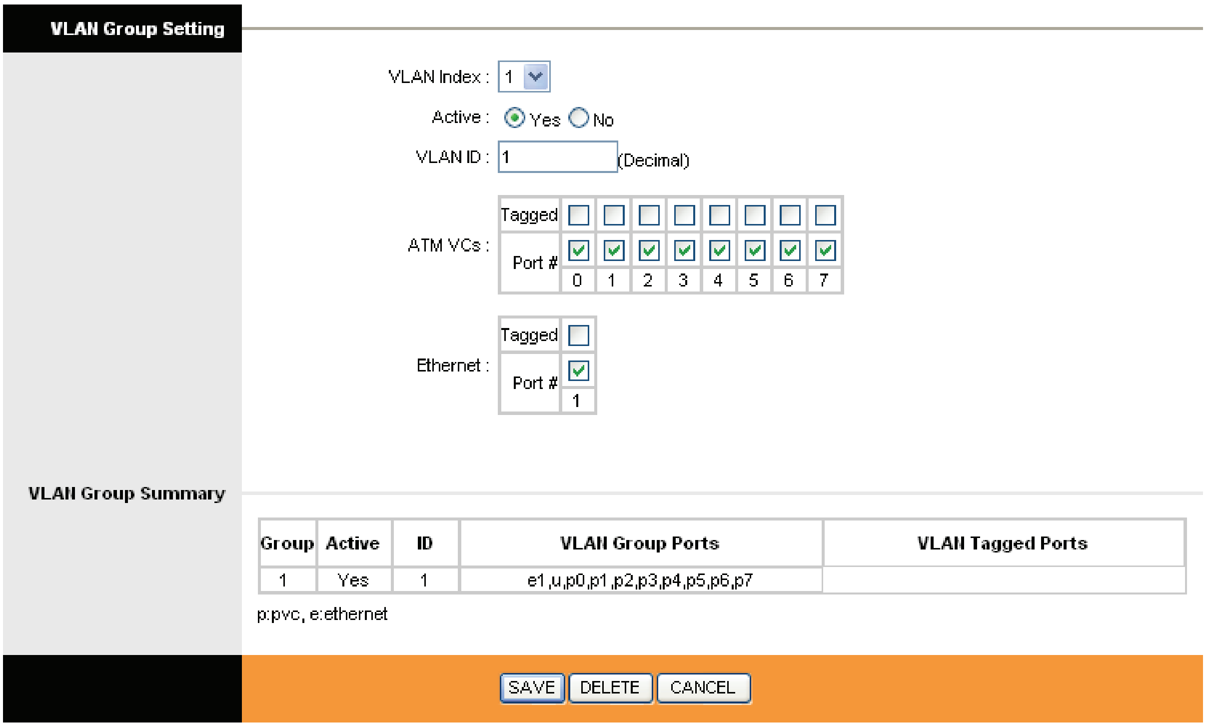


Figure 4-23

- **VLAN Index:** Select the VLAN index for this VC. You can specify 8 groups in maximum.
- **VLAN ID:** This indicates the VLAN group.
- **ATM VCs:** Select the ATM VCs as members of VLAN, and if you leave the Tagged blank, the tag in frames will be deleted when transmitted from the VC.
- **Ethernet:** Select the Ethernet port as a member of VLAN, and if you leave the Tagged blank, the tag in frames will be deleted when transmitted from the port.
- **VLAN Group Summary:** This displays the information about the VLAN Groups.

4.4.6 ADSL

Choose "**Advanced Setup→ADSL**", you can select the ADSL Type and ADSL Mode in the next screen. The ADSL feature can be selected when you meet the physical connection problem. Please check the proper settings with your Internet service provider.

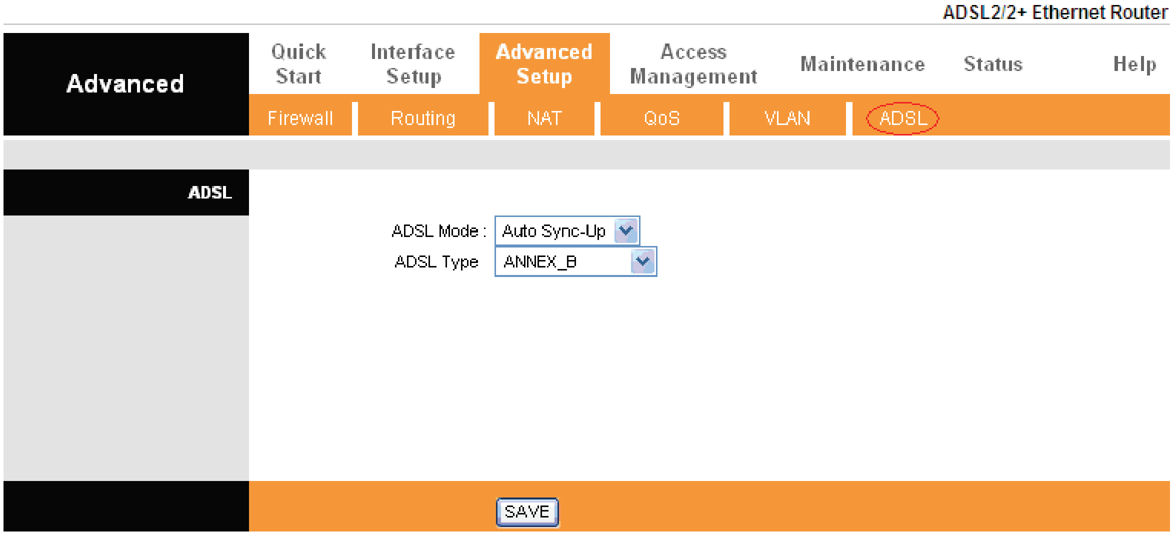


Figure 4-24

- **ADSL Mode:** Select the ADSL operation mode which your ADSL connection uses.
- **ADSL Type:** Select the ADSL operation type which your ADSL connection uses.

4.5 Access Management

Choose "**Access Management**", you can see the next submenus:



Figure 4-25

Click any of them, and you will be able to configure the corresponding function.

4.5.1 ACL

Choose "**Access Management→ACL**", you can see the next screen (shown in Figure 4-26). You can specify the client to access the ADSL Router once setting his IP as a Secure IP Address through selected applications.

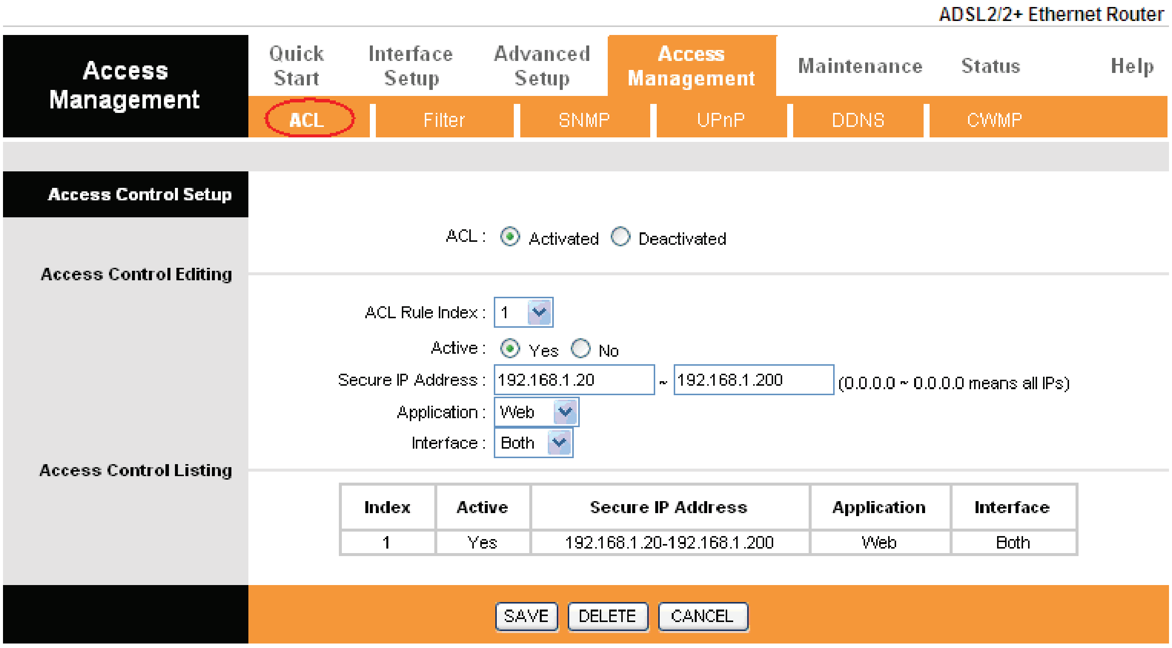


Figure 4-26

- **ACL:** If **Activated**, the IP addresses which are contained in the Access Control List can access to the Router. If **Deactivated**, all IP addresses can access to the Router.
- **ACL Rule Index:** Select the ACL rule index for the entry.
- **Active:** Enable the ACL rule.
- **Secure IP Address:** Select the IP addresses which are permitted to access to the Router remotely. With the default IP 0.0.0.0, any client would be allowed to remotely access the ADSL Router.
- **Application:** Select the application for the ACL rule, and then you can access the Router through it.
- **Interface:** Select the interface for access: LAN, WAN or Both.
- **Access Control of Listing:** This displays the information about the ACL Rules.

4.5.2 Filter

Choose "**Access Management→Filter**", you can see the Filter screen (the default is IP/MAC Filter screen shown in). The filtering feature includes IP/MAC Filter, Application Filter, URL Filter. The feature makes it possible for administrators to control user's access to the Internet, protect the networks.

4.5.2.1. IP Filter

Select **IP/Mac Filter** as the Filter type, and select **IP** as the Rule type (shown in Figure 4-27), then you can configure the filter rules based on IP address. The filtering includes **Outgoing** and **Incoming**, the detailed descriptions are provided below.



Figure 4-27

- **Filter Type Selection:** Select the filter type for the next configuration.
- **IP/MAC Filter Set Index:** Select the Set index for the IP Filter entry. This index can match with six IP / MAC Filter Rule Indexes.
- **Interface:** Select the interface for the entry.
- **Direction:** Select the direction for this IP Filter rule. There are three filtering directions: Both, Incoming, Outgoing.

Note:

Selecting **Outgoing**, the filtering feature only allows some IP traffic from LAN to access to some specifically addresses. Selecting **Incoming**, the filtering feature only allows some IP traffic from WAN to access to some specifically addresses; Selecting **Both**, the IP traffic from LAN and WAN are both blocked. By default, all outgoing IP traffic from LAN is blocked, but some IP traffic can be

allowed by setting up filters.

- **IP/MAC Filter Rule Index:** Select the Rule index for the IP Filter entry.

☞ **Note:**

You should set the **IP/MAC Filter Set Index** and **IP/MAC Filter Rule Index** together to appoint the address (shown in the Filter List) for the IP Filter rule. For example, (1, 2), it means the rule will be shown in the row 2 for the matching with 1.

- **Rule Type:** For IP Filter, please select IP here.
- **Active:** Select “Yes” to make the rule to take effect.
- **Source IP Address:** Enter the source IP address for the rule. You can enter 0.0.0.0; it means that all IP addresses are controlled by the rule.
- **Subnet Mask:** Enter the Subnet Mask for the rule.
- **Port Number:** Enter the Port Number for the rule. You can enter 0, it means that all ports are controlled by the rule.
- **Protocol:** Select the protocol: **TCP**, **UDP** or **ICMP** for the filter rule.
- **Rule Unmatched:** If the current rule can not match, and you select **Forward**, the router will skip the rule and transmit directly. If you select **Next**, the router will find the next filter rule (show in Filter list) to match.
- **IP/MAC Filter Listing:** This displays the information about the IP Filter rules.

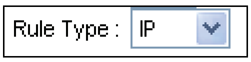
To add an IP Address filtering entry:

For example: If you desire to block E-mail received and sent by the IP address 192.168.1.7 on your local network; And wish to make the PCs with IP address 192.168.1.8 unable to visit the website of IP address 202.96.134.12, while other PCs have no limit. You can configure the rules as follows. Presume the rules are both aimed at the interface PVC0, and their indexes are (1, 1), (1, 2) and (1, 3).

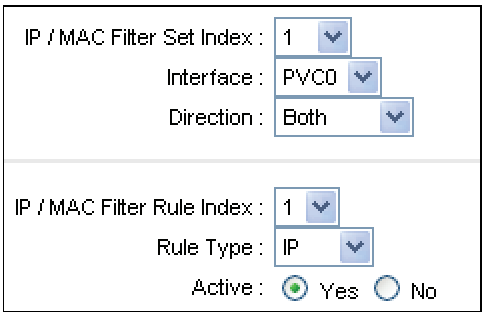
Step 1: Select the “IP/MAC Filter” as the Filer Type Selection (show in Figure 4-27).



Select the “IP” as the Rule Type on the Filter screen, then you can configure the specific rule for the example.



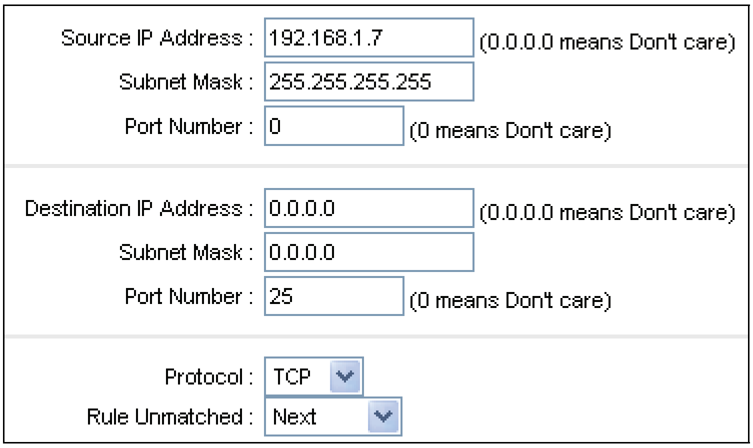
Step 2: Select the **IP/MAC Filter Set Index** and **IP/MAC Filter Rule Index** for the rule, then select the Interface “PVC0”, and select the Direction “Both” for the first rule.



Note:

If you want to make the rule take effect, please select **Yes** to active the rule.

Step 3: Enter the "Source IP Address", "Destination IP Address", "Subnet Mask" and "Port Number" in the corresponding field.



Step 4: Select the Protocol as "TCP" and select the Unmatched rule as "Next".

Step 5: Finally, click the **SAVE** to save the entry.

Step 6: Go to Step 2 to configure the next two rules: Block E-mail received by the IP address 192.168.1.7 on your local network; Make the PC with IP address 192.168.1.8 unable to visit the website of IP address 202.96.134.12.

Note:

After you complete the IP filter rules for the example, the Filter list will show as follows. You can enter the **IP / MAC Filter Set Index** to view the information about the rule.

#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	Yes	192.168.1.7/ 255.255.255.255	0.0.0.0/ 0.0.0.0	0	25	TCP	Next
2	Yes	192.168.1.7/ 255.255.255.255	0.0.0.0/ 0.0.0.0	0	110	TCP	Forward
3	Yes	192.168.1.8/ 255.255.255.255	202.96.134.12/ 255.255.255.255	0	0	TCP	Forward

Other configurations for the entries as shown in Figure 4-27:

Enter the **IP / MAC Filter Set Index** and **IP/MAC Filter Rule Index** to view or modify the entry.

Enter the **IP / MAC Filter Set Index** and **IP/MAC Filter Rule Index** to locate the specific rule, and then click the **DELETE** button to delete the entry.

4.5.2.2. MAC Filter

Select **IP/Mac Filter** as the Filter type, and select **MAC** as the Rule type (shown in Figure 4-28), then you can configure the filter rules based on MAC address.

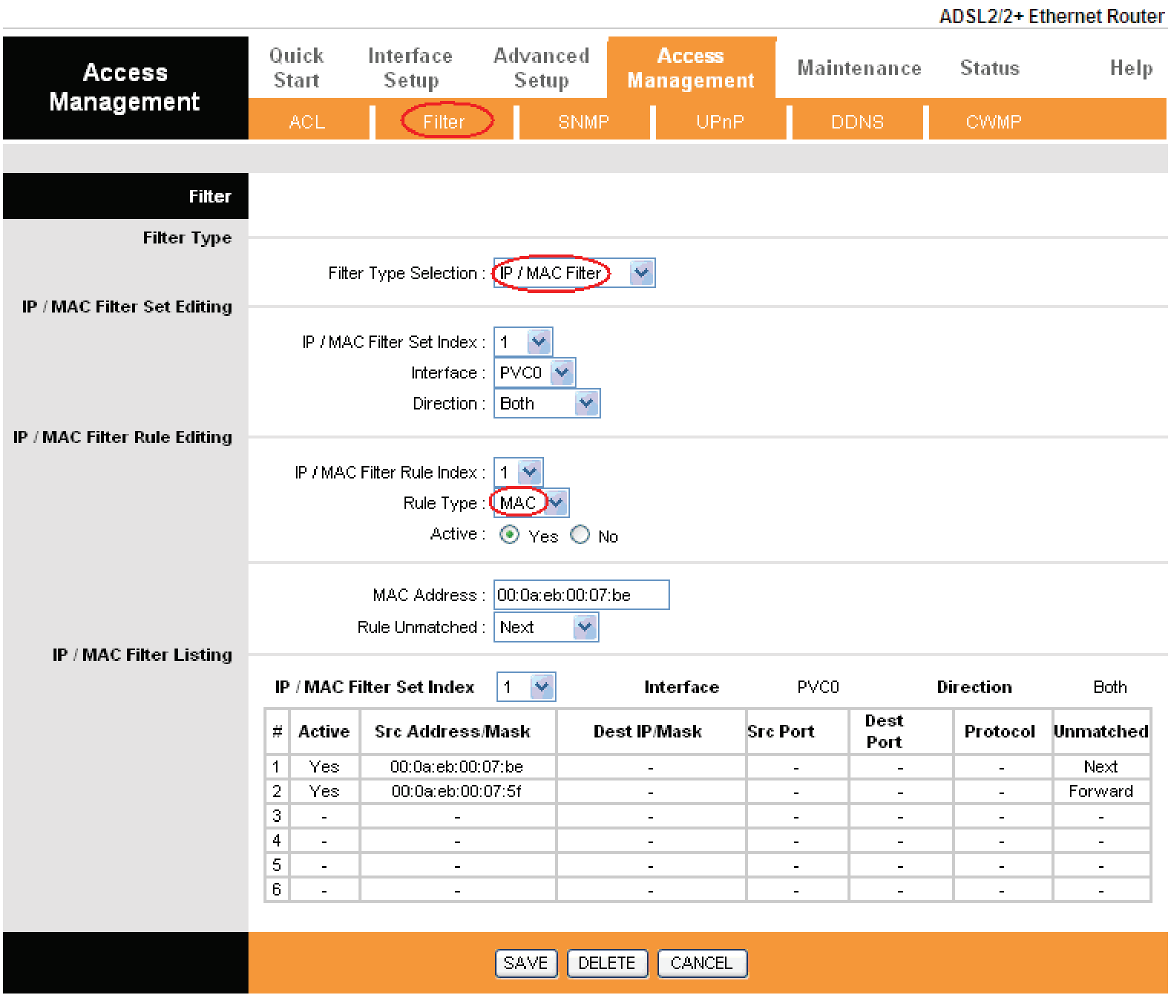


Figure 4-28

- **Rule Type:** Select MAC for the MAC Filter rule.
- **Active:** Select "Yes" to make the rule to take effect.
- **MAC Address:** Enter the MAC address for the rule.
- **Rule Unmatched:** If the current rule can not match, and you select **Forward**, the router will skip the rule and transmit directly. If you select **Next**, the router will find the next filter rule (show in Filter list) to match.
- **IP/MAC Filter Listing:** This displays the information about the MAC Filter rules.

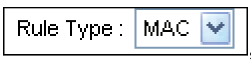
To add a MAC Address filtering entry:

For example: If you want to block the PCs with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, you can configure as follows. Presume the rules are both aimed at the interface PVC0, and their indexes are (1, 1) and (1, 2).

Step 1: Select the "IP/MAC Filter" as the Filer Type Selection:



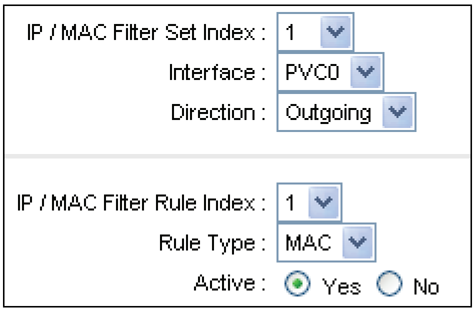
Select the "MAC" as the Rule Type on the Filter screen (show in Figure 4-28).



, Then you can configure the specific rule for the example.

Step 2: Select the **IP/MAC Filter Set Index** and **IP/MAC Filter Rule Index** for the rule, then

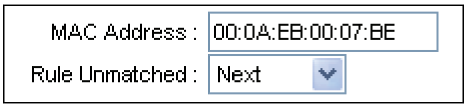
select the Interface “PVC0”, and select the Direction “Outgoing” for the first rule.



Note:

If you want to make the rule take effect, please select **Yes** to active the rule.

Step 3: Enter the “MAC Address” and select the Unmatched rule as “Next”.



Step 4: Finally, click the **SAVE** to save the entry.

Step 5: Go to Step 2 to configure the next rule: Block the PC with MAC address 00-0A-EB-00-07-5F to access the Internet.

Note:

After you complete the MAC filter rules for the example, the Filter list will show as follows. You can enter the **IP / MAC Filter Set Index** to view the information about the rule.

#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	Yes	00:0a:eb:00:07:be	-	-	-	-	Next
2	Yes	00:0a:eb:00:07:5f	-	-	-	-	Forward

Other configurations for the entries as shown in Figure 4-27:

Enter the **IP / MAC Filter Set Index** and **IP/MAC Filter Rule Index** to view or modify the entry.

Enter the **IP / MAC Filter Set Index** and **IP/MAC Filter Rule Index** to locate the specific rule, and then click the **DELETE** button to delete the entry.

4.5.2.3. Application Filter

Select **Application Filter** as the Filter type (shown in Figure 4-29), then you can configure the filter rules based on application.

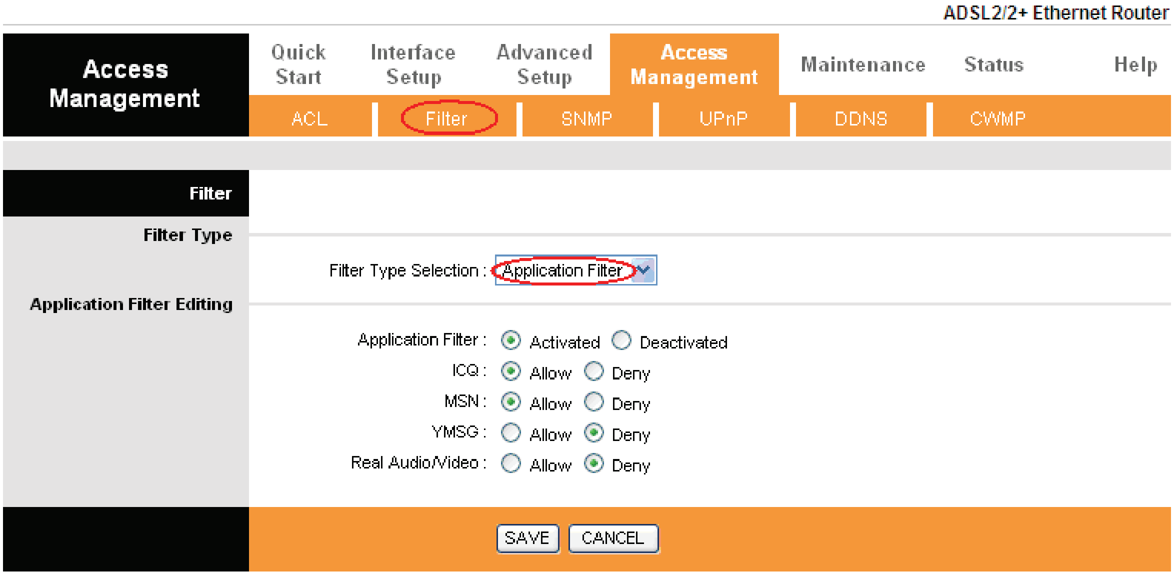


Figure 4-29

- **Filter Type Selection:** Select the Application Filter for the next configuration.
- **Application Filter:** Activate or deactivate the function.
- **ICQ & MSN & YMSG & Real Audio/Video:** Select **Allow** or **Deny** for these applications. If you select Allow, the Router will accept the application; if you select Deny, the Router will forbid the application.

4.5.2.4. URL

Select **URL** as the Filter type (shown in Figure 4-30), then you can configure the filter rules based on URL.

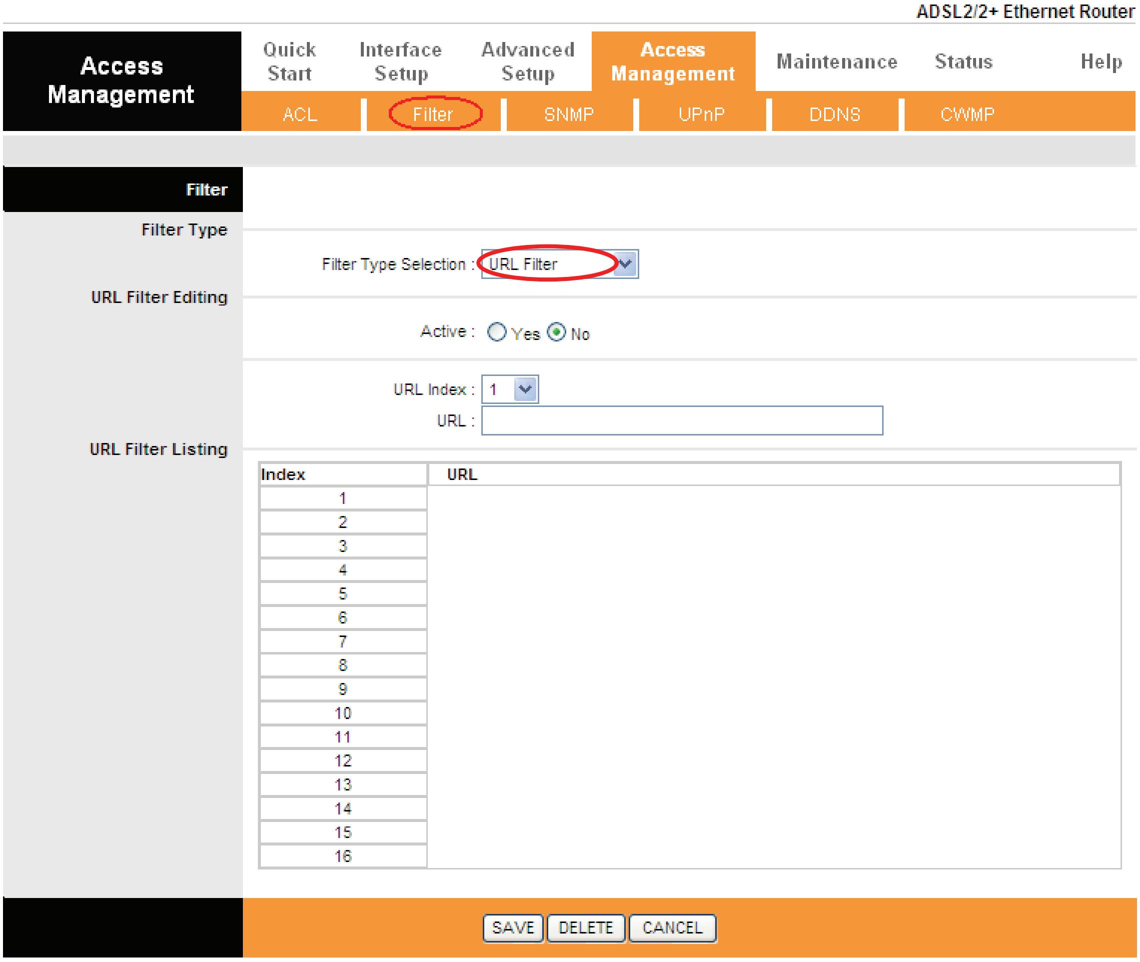


Figure 4-30

- **Filter Type Selection:** Select the URL Filter for the next configuration.
- **Active:** Select "Yes" to make the rule to take effect.
- **URL Index:** Select the index for the URL Filter entry.
- **URL:** Enter the URL for this URL Filter.
- **URL Filter Listing:** This displays the information about the URL Filter rules.

To add a URL filter entry:

For example: If you want to forbid the user to access the website: www.sina.com. Presume the rule is aimed at the interface PVC0, and its index is "1".

Step 1: Select the "URL Filter" as the Filer Type Selection (show in Figure 4-30).

Step 2: Select the Index for the rule, and then enter the website in the URL field.

Step 3: Finally, Select Yes to active the rule, and then click the **SAVE** to save the entry.

Other configurations for the entries as shown in Figure 4-27:

Enter the **URL Index** to view or modify the entry.

Enter the **URL Index** to locate the specific rule, and then click the **DELETE** button to delete the entry.

4.5.3 SNMP

Choose "**Access Management→SNMP**", you can see the SNMP screen. The Simple Network

Management Protocol (SNMP) is used for exchanging information between network devices.

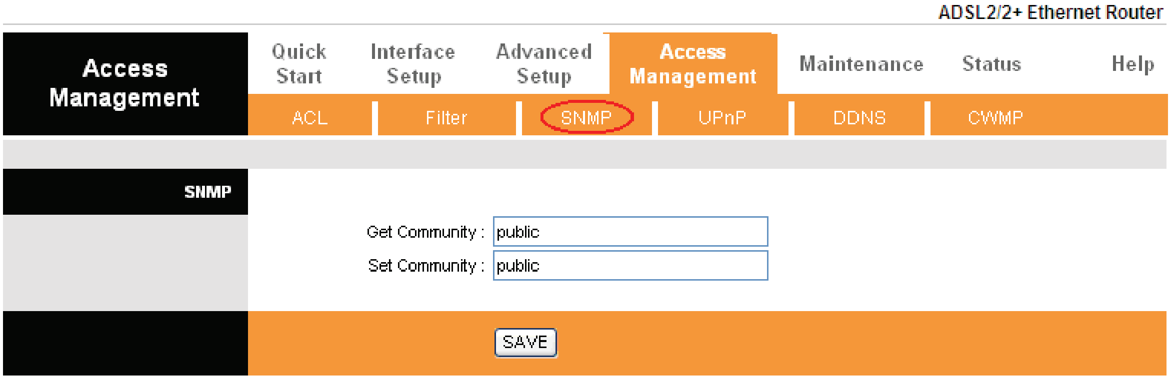


Figure 4-31

- **Get Community:** Select to set the password for the incoming Get and Get next requests from the management station.
- **Set Community:** Select to set the password for incoming Set requests from the management station.

4.5.4 UPnP

Choose "**Access Management→UPnP**", you can configure the UPnP in the screen (shown in Figure 4-32).

UPnP (Universal Plug and Play) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. An UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. UPnP broadcasts are only allowed on the LAN.

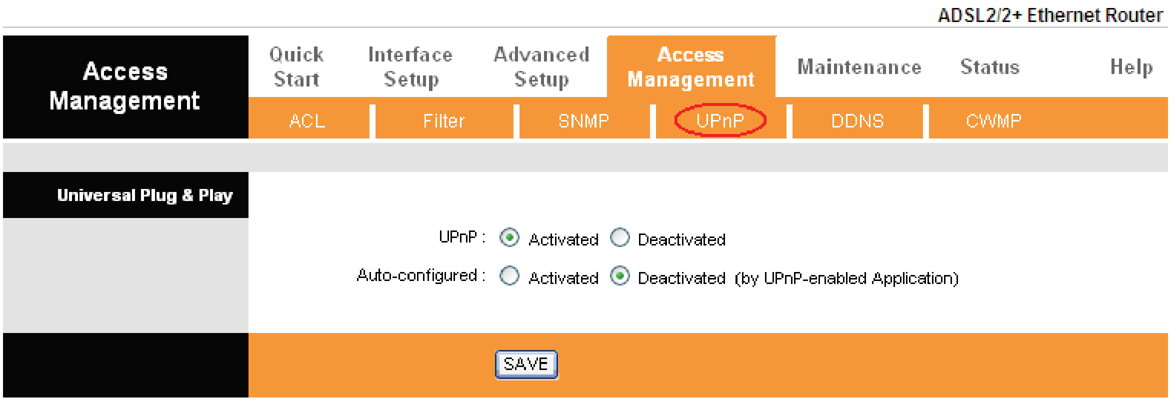


Figure 4-32

- **UPnP:** Activate or Deactivate the UPnP function. Only when the function is activated, can the UPnP take effect.
- **Auto-Configure:** If you activate the function, then the UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions.

4.5.5 DDNS

Choose "**Access Management→DDNS**", you can configure the DDNS function in the screen (shown in Figure 4-33).

The router offers a Dynamic Domain Name System (**DDNS**) feature. The feature lets you use a static host name with a dynamic IP address. User should type the host name, user name and password assigned to your ADSL Router by your Dynamic DNS provider. User also can decide to turn on DYNDNS Wildcard or not.

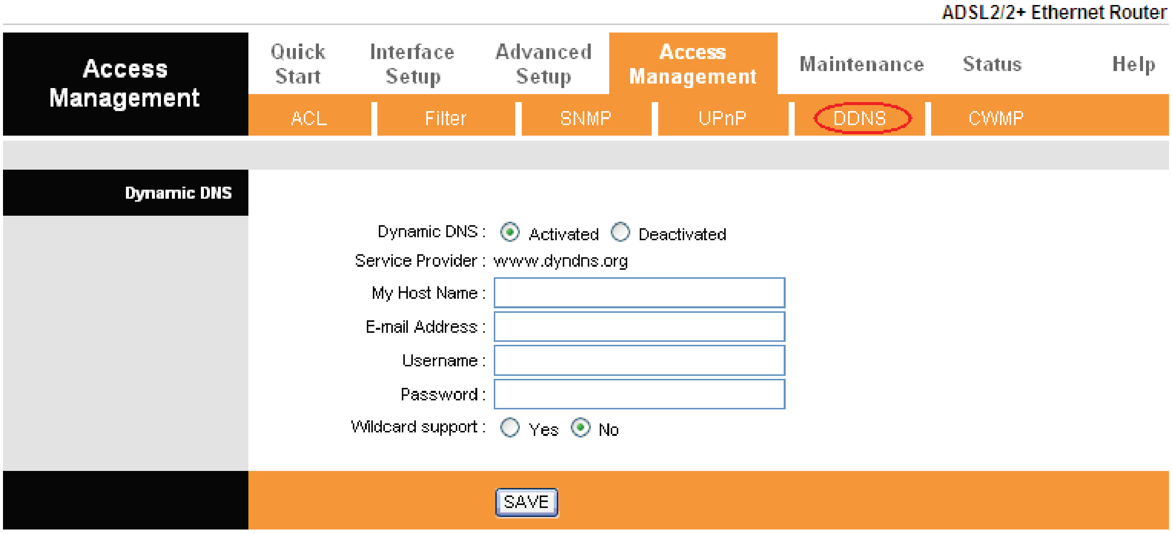


Figure 4-33

- **Dynamic DNS:** Activate the DDNS function or not.
- **Service Provider:** This field displays the service provider of DDNS.
- **My Host Name:** Enter your host name here.
- **E-mail Address:** Enter your E-mail address here.
- **Username & Password:** Type the "User Name" and "Password" for your DDNS account.
- **Wildcard support:** Select the option to use Wildcard function

4.5.6 CWMP

Choose "**Access Management→CWMP**", you can configure the CWMP function in the screen (shown in Figure 4-34).

The router offers CWMP feature. The function supports TR-069 protocol which collects information, diagnoses the devices and configures the devices automatically via ACS (Auto-Configuration Server).

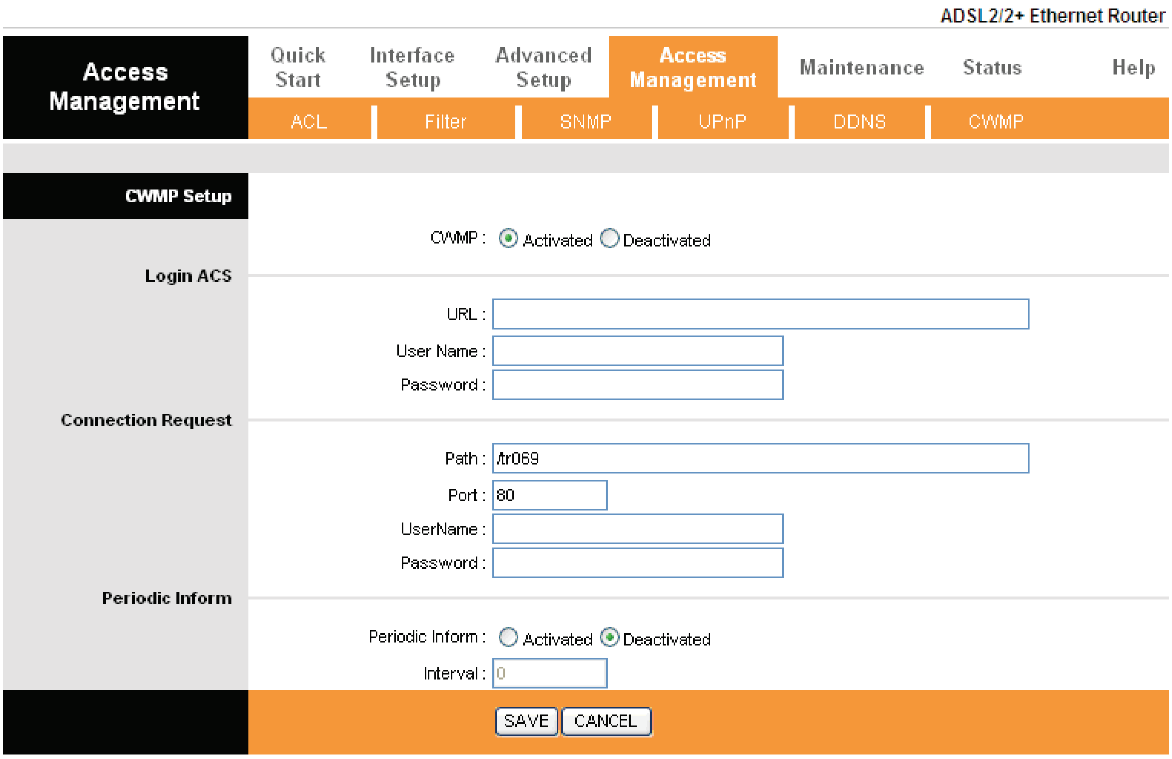


Figure 4-34

- **CWMP:** Select activate the CWMP function.
- **URL:** Enter the website of ACS which is provided by your ISP.
- **User Name/Password:** Enter the User Name and password to login the ACS server.
- **Path:** Enter the path that connects to the ACS server.
- **Port:** Enter the port that connects to the ACS server.
- **User Name/Password:** Enter the User Name and Password that provided the ACS server to login the router.
- **Periodic Inform:** Activate or deactivate the function. If Activated, the information will be informed to ACS server periodically.
- **Interval:** Enter the interval time here.

4.6 Maintenance

Choose "**Maintenance**", you can see the next submenus:



Figure 4-35

Click any of them, and you will be able to configure the corresponding function.

4.6.1 Administration

Choose "**Maintenance→Administration**", you can set new password for admin in the screen

(shown in Figure 4-36).

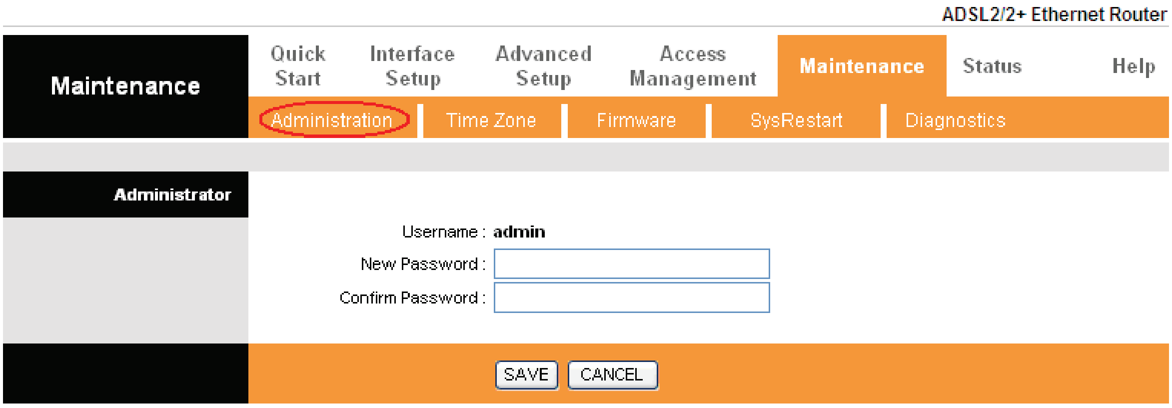


Figure 4-36

Note:

1) There is only one account that can access Web-Management interface. The default account is "admin", and the password is "admin". Admin has read/write access privilege.
2) When you change the password, you should enter the new password twice, and then click **SAVE** to make the new password take effect.

4.6.2 Time Zone

Choose "**Maintenance→Time Zone**", you can configure the system time in the screen (shown in Figure 4-36).

The system time is the time used by the device for scheduling services. There are three methods to configure the time. You can manually set the time or connect to a NTP (Network Time Protocol) server. If a NTP server is set, you will only need to set the time zone. If you manually set the time, you may also set Daylight Saving dates and the system time will automatically adjust on those dates.

1. NTP Server automatically

Select **NTP Server automatically** as the Synchronize time, you only need to set the time zone.

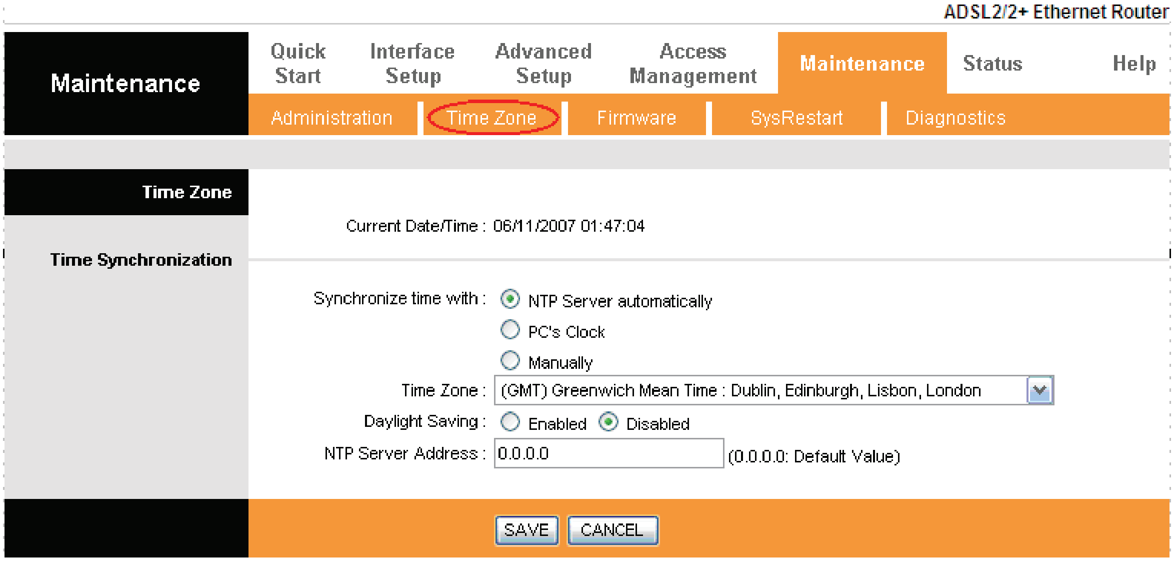


Figure 4-37

Note:

The ADSL Router built-in some NTP Servers, when the Router connects to the Internet, the Router will get the system time automatically from the NTP Server. You can also configure the NTP Server address automatically, and then the Router will get the time from the specific Server firstly.

2. PC's Clock

Select **PC's Clock** as the Synchronize time, you don't need to set any items.

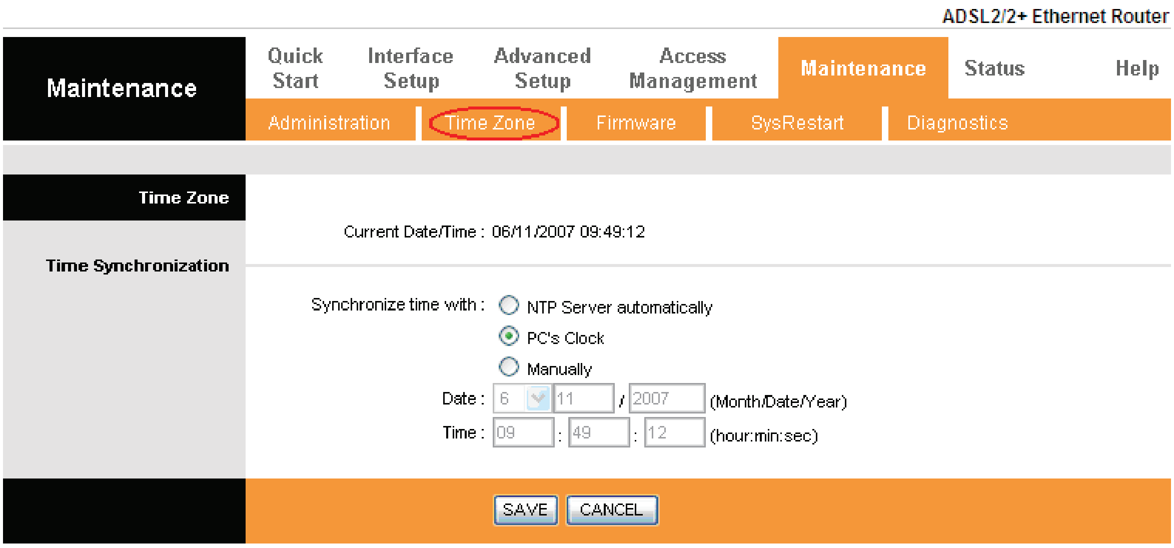


Figure 4-38

3. Manually

Select **Manually** as the Synchronize time, you need to set the date and time corresponding to the current time.

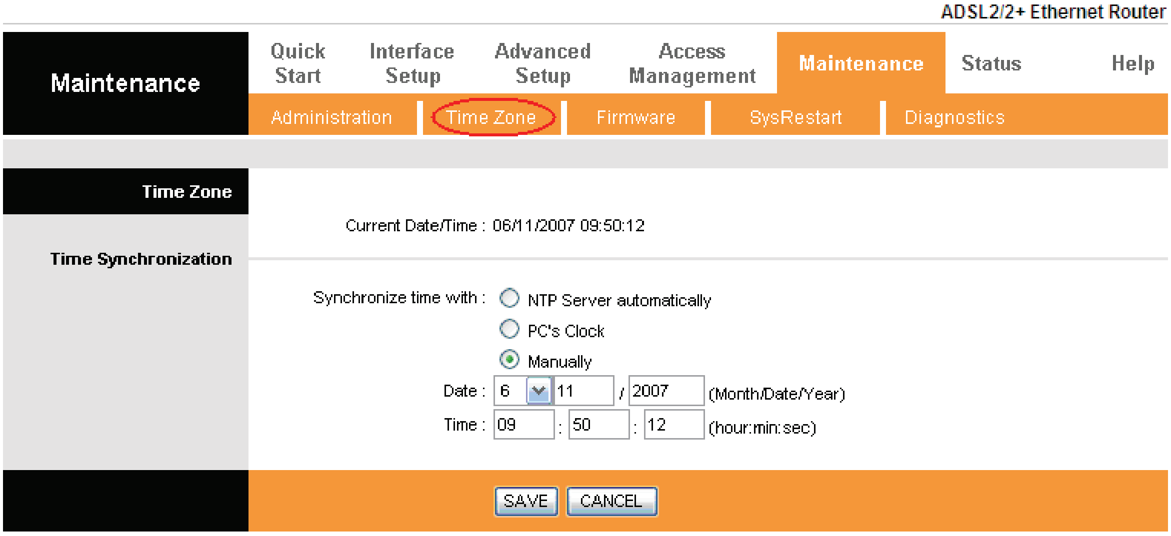


Figure 4-39

4.6.3 Firmware

Choose "**Maintenance→Firmware**", you can upgrade the firmware of the Router in the screen (shown in Figure 4-40). Make sure the firmware or romfile you want to use is on the local hard drive of the computer. Click **Browse** to find the local hard drive and locate the firmware or romfile to be used for upgrade.

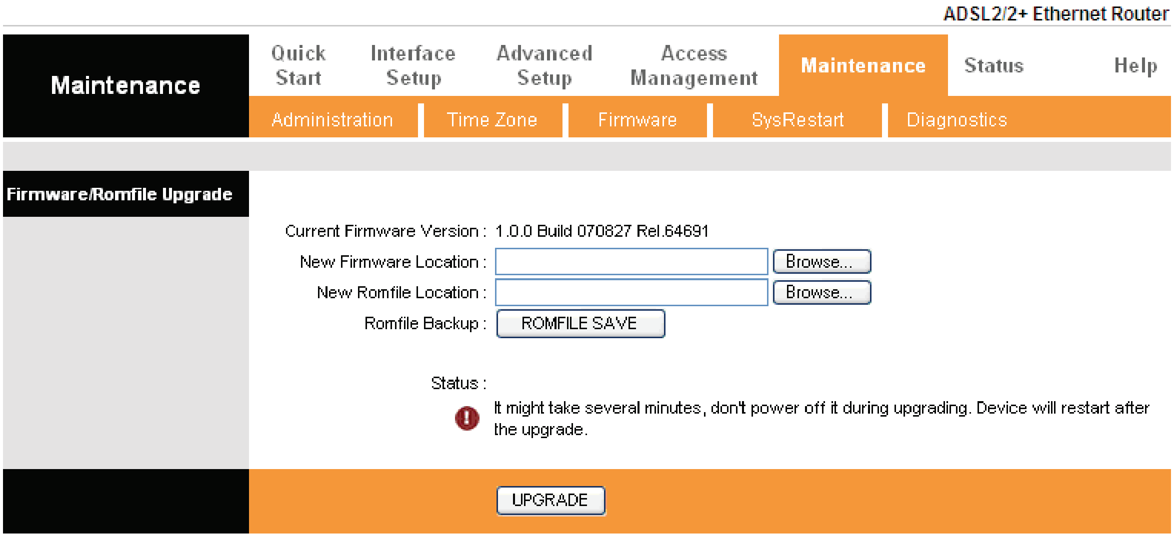


Figure 4-40

To upgrade the router's firmware, follow these instructions below:

Step 1: Download a more recent firmware upgrade file from the TP-LINK website (www.tp-link.com).

Step 2: Type the path and file name of the update file into the "New Firmware Location" field. Or click the **Browse** button to locate the update file.

Step 3: Click the **UPGRADE** button.

Note:

1) New firmware versions are posted at www.tp-link.com and can be downloaded for free. If

the router is not experiencing difficulties, there is no need to download a more recent firmware version, unless the version has a new feature that you want to use.

2) When you upgrade the router's firmware, you may lose its current configurations, so please back up the router's current settings before you upgrade its firmware.
3) Do not turn off the router or press the Reset button while the firmware is being upgraded.
4) The router will reboot after the upgrading has been finished.

To back up the Router's current settings:

Step 1: Click the **ROMFILE SAVE** button (shown in Figure 4-40), click **Save** button in the next screen (shown in Figure 4-41) to proceed.

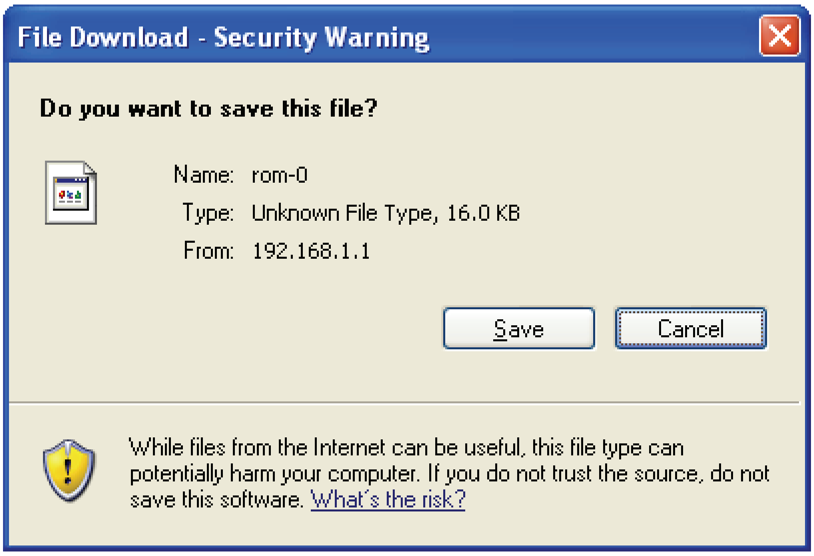


Figure 4-41

Step 2: Save the file as the appointed file (shown in Figure 4-42).

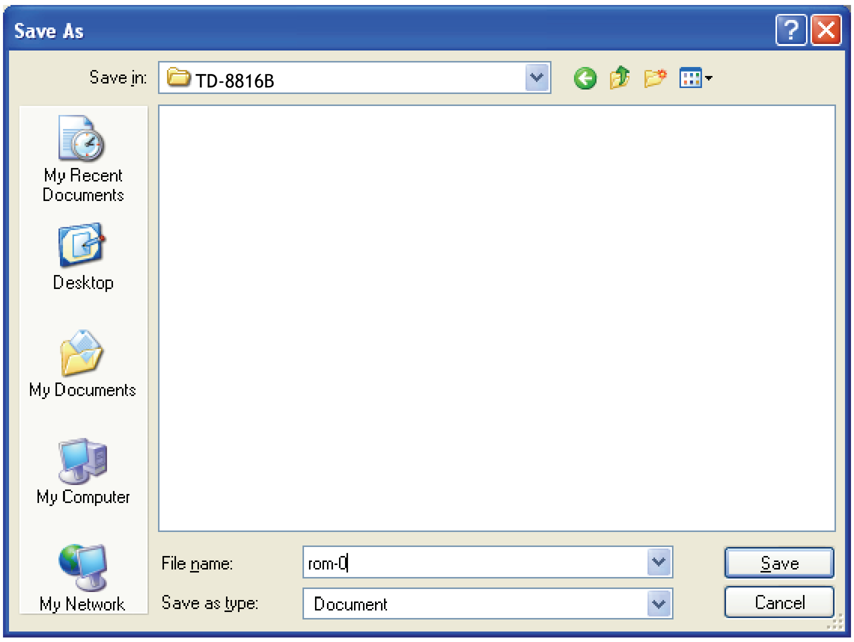


Figure 4-42

To restore the Router's settings:

Step 1: Click the **Browse** button to locate the update file for the device, or enter the exact path in "New Romfile Location" field.

Step 2: Click the **UPGRADE** button to complete.

4.6.4 System Restart

Choose "**Maintenance→System Restart**", you can select to restart the device with current settings or restore to factory default settings in the screen (shown in Figure 4-43).

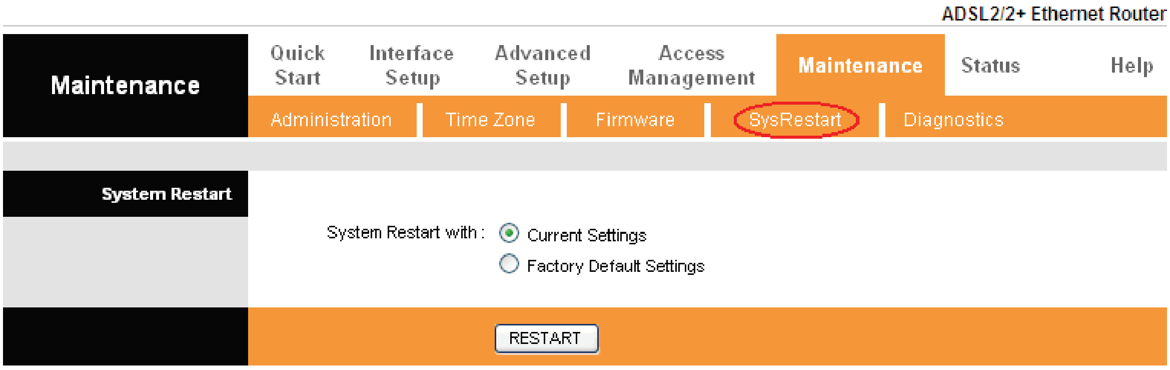


Figure 4-43

4.6.5 Diagnostic

Choose "**Maintenance→Diagnostic**", you can view the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides in the screen (shown in Figure 4-44).

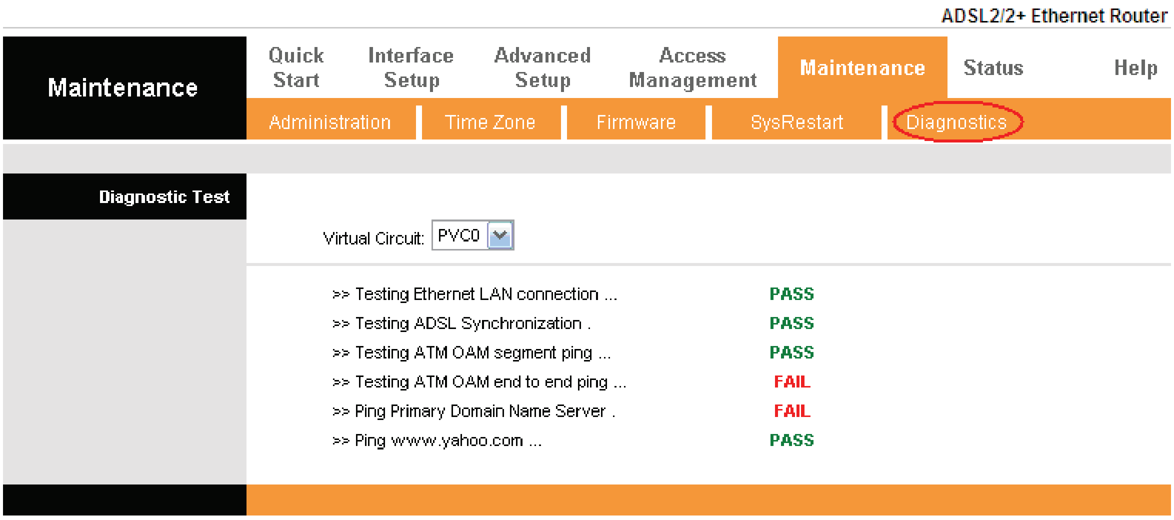


Figure 4-44

4.7 Help

Choose "**Help**", you can view the help information for configuration of any function.

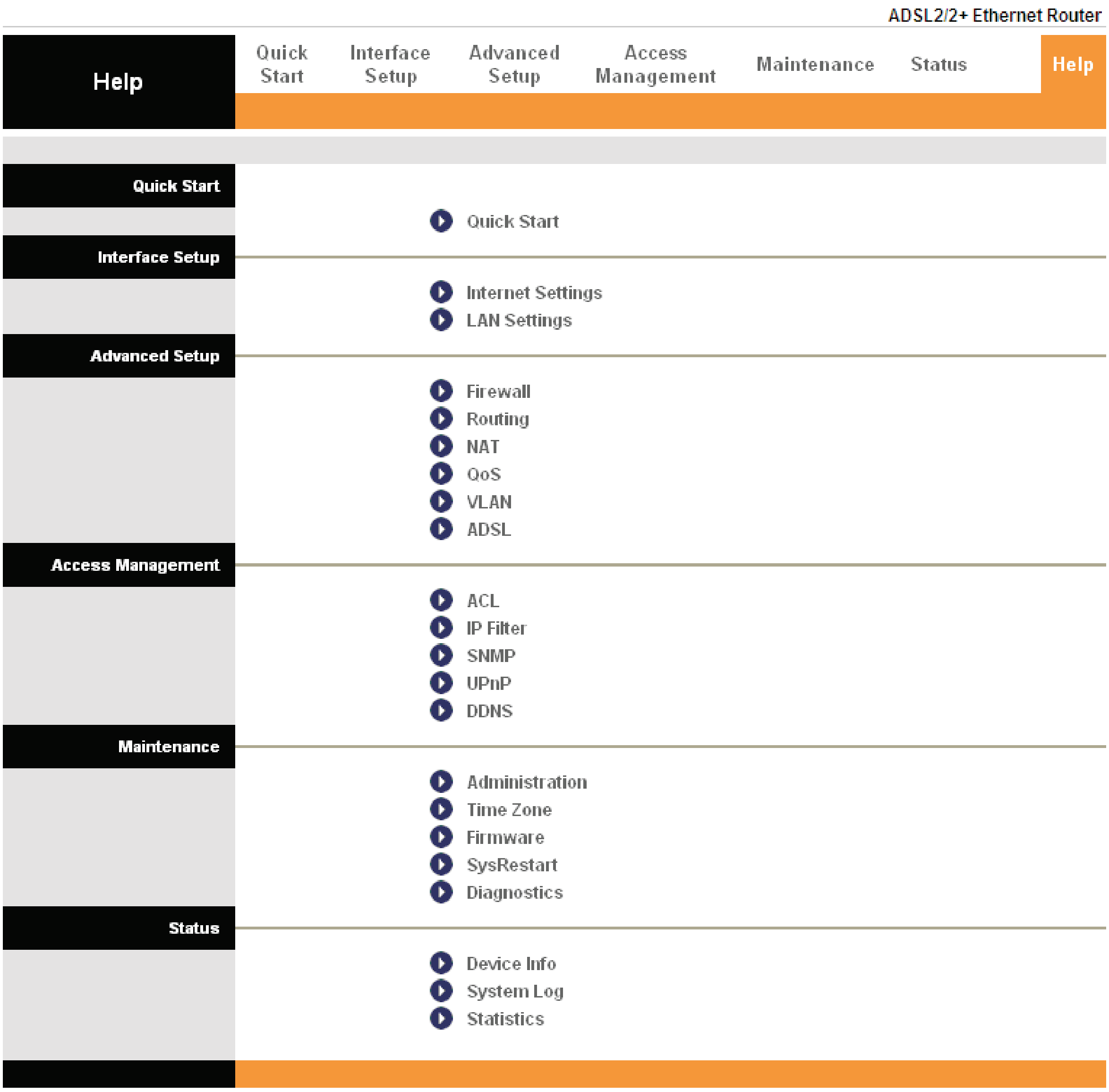


Figure 4-45

Note:

Click the tab, and you will be able to get the corresponding information.

Appendix A: Specification

General	
Standards and Protocols	ANSI T1.413, ITU G.992.1, ITU G.992.2, ITU G.992.3, ITU G.992.5 IEEE 802.3, IEEE 802.3u, TCP/IP, PPPoA , PPPoE, SNTP, HTTP, DHCP, ICMP, NAT,CWMP
Safety & Emission	FCC、CE
Ports	1 10/100M Auto-Negotiation RJ45 port（Auto MDI/MDIX) 1 RJ11 port
LEDs	LAN, ADSL Power, ACT
Network Medium	10Base-T: UTP category 3, 4, 5 cable 100Base-TX: UTP category-5 Max line length: 6.5Km
Data Rates	Downstream: Up to 24Mbps Upstream: Up to 3.5Mbps（With Annex M enabled）
System Requirement	Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later Win 9x/ME/2000/XP/Vista
Physical and Environment	
Working Temperature	0℃ ~40℃
Working Humidity	10% ~ 90% RH (non-condensing)
Storage Temperature	-40℃ ~ 70℃
Storage Humidity	5% ~ 90% RH (non-condensing)